(19) JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: **11275157 A**

(43) Date of publication of application: **08.10.99**

(51) Int. Cl **H04L 12/66**
H04Q 7/38
H04L 12/28
H04L 12/46
H04L 12/14
H04L 12/56
H04M 3/00
H04M 11/00

(21) Application number: **10306445**

(22) Date of filing: **14.10.98**

(30) Priority: **14.10.97 US 97 61915**
24.08.98 US 98 138683

(71) Applicant: **LUCENT TECHNOL INC**

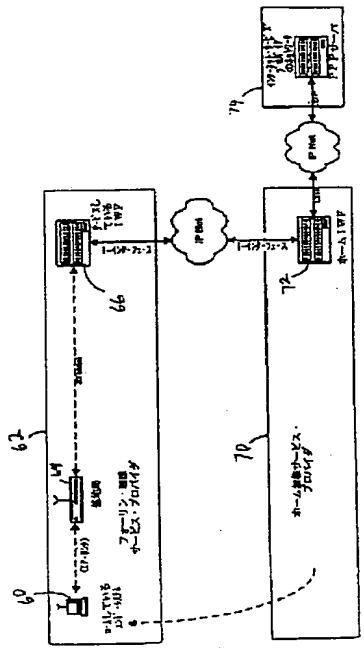
(72) Inventor: **CHUAH MOOI CHOO**
RAI GIRISH

(54) **OPTIMUM ROUTING SYSTEM**

(57) Abstract:

PROBLEM TO BE SOLVED: To optimize routing to a requested communications server of a mobile end system.

SOLUTION: A network integrates an MAC(medium access control) hand-off message with a network hand-off message and separately allocates a registration function to a registration server and a routing function to an inter-working unit. The network provides an intermediate XTunnel channel between a radio hub and an inter-working function unit 66 inside a foreign network, and provides an I-XTunnel channel between the inter-working function unit inside the foreign network and the inter-working function unit 72 inside a home network. The network reinforces a layer 2 tunneling protocol so as to support a mobile end system, and registration of a network layer is executed before starting a PPP (point-to-point protocol) communication session.



(19)日本国特許庁（ＪＰ）　(12)**公開特許公報**（Ａ）　(11)特許出願公開番号

特開平11－275157

(43)公開日　平成11年(1999)10月８日

(51)Int.Cl.[6]	識別記号	ＦＩ	
Ｈ０４Ｌ　12/66		Ｈ０４Ｌ　11/20	Ｂ
Ｈ０４Ｑ　7/38		Ｈ０４Ｍ　3/00	Ｂ
Ｈ０４Ｌ　12/28		11/00	３０３
12/46		Ｈ０４Ｂ　7/26	１０９Ｍ
12/14		Ｈ０４Ｌ　11/00	３１０Ｂ

審査請求　未請求　請求項の数14　ＯＬ　外国語出願　（全181頁）　最終頁に続く

(21)出願番号　特願平10－306445

(22)出願日　平成10年(1998)10月14日

(31)優先権主張番号　６０／０６１９１５

(32)優先日　1997年10月14日

(33)優先権主張国　米国（ＵＳ）

(31)優先権主張番号　０９／１３８６８３

(32)優先日　1998年８月24日

(33)優先権主張国　米国（ＵＳ）

(71)出願人　596092698
ルーセント　テクノロジーズ　インコーポレーテッド
アメリカ合衆国．07974－0636　ニュージャーシィ，マレイ　ヒル，マウンテン　アヴェニュー　600

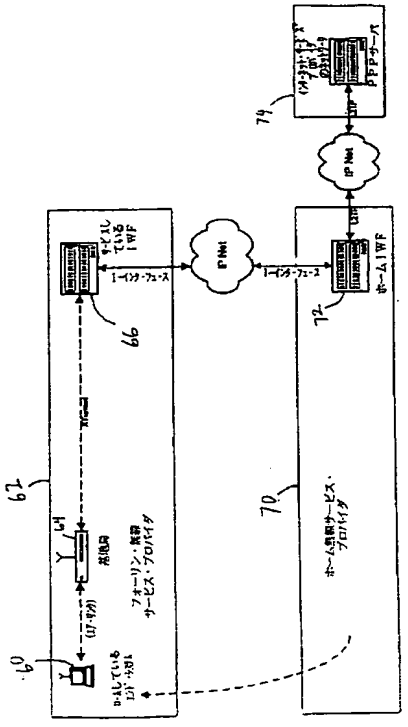
(72)発明者　ムーイ　チョー　チュアー
アメリカ合衆国　07724　ニュージャーシィ，イートンタウン，イートンクレスト　ドライヴ　184ビー

(74)代理人　弁理士　岡部　正夫　（外11名）

最終頁に続く

(54)【発明の名称】　最適ルーティングシステム

(57)【要約】　（修正有）
【課題】モバイルエンドシステムの要求される通信サーバへのルーティングの最適化を行う。
【解決手段】ネットワークはMACハンドオフメッセージをネットワークハンドオフメッセージと統合し、別個に、登録機能を登録サーバに、ルーティング機能をインターワーキングユニットに割り当てる。ネットワークはフォーリンネットワーク内の無線ハブとインターワーキング機能ユニット６６との間に中間XTunnelチャネルを提供し、フォーリンネットワーク内のインターワーキング機能ユニットとホームネットワーク内のインターワーキング機能ユニット７２の間にI-XTunnelチャネルを提供する。ネットワークは層２トンネリングプロトコルをモバイルエンドシステムがサポートできるように強化し、ネットワーク層の登録をPPP通信セッションを開始する前に遂行する。



【特許請求の範囲】

【請求項１】　結合されたデータネットワークであって、このデータネットワークが：フォーリンネットワークとホームネットワークを含み、

前記フォーリンネットワークが基地局、無線ハブ、サービング登録サーバを備えるフォーリンモバイル交換センタ、およびサービングインターワーキング機能を含み、

前記ホームネットワークがホーム登録サーバを備えるホームモバイルセンタおよびホームインターワーキング機能を含み、このデータネットワークがさらに前記ホームネットワークに加入し、前記フォーリンネットワーク内で動作しているエンドシステムを含み、このエンドシステムが登録リクエストを生成するエンドシステム登録エージェントを含み、前記登録リクエストが要求される通信サーバを備える要求される通信ネットワークの指標を含み、前記エンドシステムが前記登録リクエストを前記サービング登録サーバに送信し、前記サービング登録サーバが第一のモジュールを含み、これが前記登録リクエストを処理することで、前記要求される通信サーバとホームインターワーキング機能かサービングインターワーキング機能のどちらか一つの間の最適なルートを決定し、前記サービング登録サーバがさらに第二のモジュールを含み、これが前記第一のモジュールが前記最適なルートが前記サービングインターワーキング機能と前記要求される通信サーバとの間であることを決定した場合、前記サービングインターワーキング機能を前記要求される通信サーバにリンクすることを特徴とするデータネットワーク。

【請求項２】　前記サービング登録サーバがさらに第三のモジュールを含み、これが前記ホーム登録サーバに向けて前記登録リクエストを、前記サービング登録サーバが前記サービングインターワーキング機能を前記要求される通信サーバにリンクしたことを示す指標を付加して送信することを特徴とする請求項１のデータネットワーク。

【請求項３】　前記要求される通信サーバが前記要求される通信ネットワーク内の複数の通信サーバの内の一つの通信サーバであり；前記第一のモジュールが前記複数の通信サーバの中から前記要求される通信サーバを決定するためのサブモジュールを含むことを特徴とする請求項１のデータネットワーク。

【請求項４】　前記ホームネットワークと前記フォーリンネットワークが、前記エンドシステムが前記フォーリンネットワーク内で動作しているとき、前記エンドシステムに対して課金情報を共有することを特徴とする請求項１のデータネットワーク。

【請求項５】　結合されたデータネットワークであって、このデータネットワークが：フォーリンネットワークとホームネットワークを含み、

前記フォーリンネットワークが、基地局およびサービング登録サーバを備えるフォーリンモバイル交換センタを含み、前記基地局がサービングインターワーキング機能を備えるアクセスハブを含み、

前記ホームネットワークが、ホーム登録サーバを備えるホームモバイルセンタおよびホームインターワーキング機能を含み、このデータネットワークがさらに前記ホームネットワークに加入し、前記フォーリンネットワーク内で動作しているエンドシステムを含み、このエンドシステムが登録リクエストを生成するエンドシステム登録エージェントを含み、前記登録リクエストが要求される通信サーバを備える要求される通信ネットワークの指標を含み、前記エンドシステムが前記登録リクエストを前記サービング登録サーバに送信し、前記サービング登録サーバが第一のモジュールを含み、これが前記登録リクエストを処理することで、前記要求される通信サーバとホームインターワーキング機能かサービングインターワーキング機能のいずれか一つとの間の最適なルートを決定し、前記サービング登録サーバがさらに第二のモジュールを含み、これが前記ホーム登録サーバに向けて前記登録リクエストを、前記サービング登録サーバによって前記最適なルートが前記サービングインターワーキング機能と前記要求される通信サーバとの間であることが決定されたことを示す第一の指標およびルート最適化が希望されることを示す第二の指標を付加して送信することを特徴とするデータネットワーク。

【請求項６】　前記要求される通信サーバが前記要求される通信ネットワーク内の複数の通信サーバの内の一つの通信サーバであり；前記第一のモジュールが前記複数の通信サーバの中から前記要求される通信サーバを決定（選択）するためのサブモジュールを含むことを特徴とする請求項５のデータネットワーク。

【請求項７】　前記サービング登録サーバが第三のモジュールを含み、これが前記登録リクエストを前記第一および第二の付加された指標と共に前記ホーム登録サーバに送信した後に、前記サービングインターワーキング機能と前記要求される通信プロセッサ（通信サーバ）との間にリンクを確立することを特徴とする請求項５のデータネットワーク。

【請求項８】　前記ホーム登録サーバがさらに第四のモジュールを含み、これが前記サービングインターワーキング機能と前記要求される通信サーバとの間の前記リンクが認証（検証）されたことを示す指標を含む登録応答を前記登録サーバに送り返し；前記ホーム登録サーバがさらに第五のモジュールを含み、これが前記ホームインターワーキング機能に対して、リンク状態を前記サービングインターワーキング機能に転送することを指令することを特徴とする請求項７のデータネットワーク。

【請求項９】　前記ホームネットワークと前記フォーリンネットワークが、前記エンドシステムが前記フォーリンネットワーク内で動作しているとき、前記エンドシス

テムに対して課金情報を共有することを特徴とする請求項５のデータネットワーク。

【請求項１０】　結合されたデータネットワーク内で用いるルーティングを最適化する方法であって、前記データネットワークがフォーリンネットワークとホームネットワークを含み、前記フォーリンネットワークが基地局およびサービング登録サーバを備えるフォーリンモバイル交換センタを含み、前記基地局がサービングインターワーキング機能を備えるアクセスハブを含み、前記ホームネットワークがホーム登録サーバを備えるホームモバイルセンタおよびホームインターワーキング機能を含み、前記データネットワークがさらに前記ホームネットワークに加入し、前記フォーリンネットワーク内で動作しているエンドシステムを含み、前記エンドシステムが登録リクエストを生成するエンドシステム登録エージェントを含み、この方法が：前記エンドシステムの所で登録リクエストを生成するステップを含み、この登録リクエストが要求される通信サーバを備える要求される通信ネットワークの指標を含み；この方法がさらに前記エンドシステムから前記登録リクエストを前記サービング登録サーバに送信するステップ；前記サービング登録サーバ内の第一のモジュールによって前記登録リクエストを処理することで、前記要求される通信サーバとホームインターワーキング機能とサービングインターワーキング機能のいずれか一つとの間の最適なルートを決定するステップ；および前記第一のモジュールが前記最適なルートが前記サービングインターワーキング機能と前記要求される通信サーバとの間であることを決定した場合、前記サービングインターワーキング機能を前記要求される通信サーバにリンクするステップを含むことを特徴とする方法。

【請求項１１】　さらに：前記ホーム登録サーバに前記登録リクエストを、前記サービング登録サーバが前記サービングインターワーキング機能と前記要求される通信サーバをリンクしたことを示す指標を付加して送信するステップを含むことを特徴とする請求項１０の方法。

【請求項１２】　前記要求される通信サーバが前記要求される通信ネットワーク内の複数の通信サーバの内の一つの通信サーバであり；前記第一のモジュールが前記複数の通信サーバの中から前記要求される通信サーバを決定するためのサブモジュールを含むことを特徴とする請求項１０の方法。

【請求項１３】　前記ホームネットワークと前記フォーリンネットワークが、前記エンドシステムが前記フォーリンネットワーク内で動作しているとき、前記エンドシステムに対して課金情報を共有することを特徴とする請求項１０の方法。

【請求項１４】　結合されたデータネットワーク内で用いるルーティングを最適化する方法であって、前記データネットワークがフォーリンネットワークとホームネットワークを含み、前記フォーリンネットワークが基地局およびサービング登録サーバを備えるフォーリンモバイル交換センタを含み、前記基地局がサービングインターワーキング機能を備えるアクセスハブを含み、前記ホームネットワークがホーム登録サーバを備えるホームモバイルセンタおよびホームインターワーキング機能を含み、前記データネットワークがさらに前記ホームネットワークに加入し、前記フォーリンネットワーク内で動作しているエンドシステムを含み、前記エンドシステムが登録リクエストを生成するエンドシステム登録エージェントを含み、この方法が：前記エンドシステムの所で登録リクエストを生成するステップを含み、この登録リクエストが要求される通信サーバを備える要求される通信ネットワークの指標を含み；この方法がさらに前記エンドシステムから前記登録リクエストを前記サービング登録サーバに送信するステップ；前記サービングインターワーキング機能と前記ホームインターワーキング機能のどちらが前記要求される通信サーバに近いかを決定するステップ；前記要求される通信サーバに前記サービングインターワーキング機能の方が前記ホームインターワーキング機能より近い場合、前記サービングインターワーキング機能に対して、前記要求される通信サーバに向けてコネクションを確立することを指令するステップ；および前記ホーム登録サーバに対して、前記エンドシステムが前記サービングインターワーキング機能および前記要求される通信サーバによるサービスを受けていることを通知するステップを含むことを特徴とする方法。

【発明の詳細な説明】

【０００１】

【発明の分野】本発明は、コンピュータユーザに、インターネットおよびプライベートイントラネットへのリモートアクセスを仮想プライベートネットワークサービスを用いて高速パケット交換無線データリンクを通じて提供するパケット交換データネットワーク内でのモバイルエンドシステムの管理に関する。本発明は、より詳細には、モバイルエンドシステムの要求される通信サーバへのルーティングの最適化に関する。

【０００２】

【従来の技術】図１は、典型的には一体となってユーザモデム４を通じてユーザコンピュータ２へのリモートインターネットアクセスを提供する３つのビジネスエンティティを示す。第一のビジネスエンティティは、ダイヤルアップ式の簡単な古いタイプの電話システム（plain old telephone system、POTS）あるいはサービス統合データネットワーク（integrated services data network、ISDN）を所有および運用する電話会社である。電話会社は、公衆交換電話ネットワーク（public switched telephone network、PSTN）６の形式にてメディアを提供し、ユーザと他の２つのビジネスエンティティとの間のビット（あるいはパケット）はこの上を流れる。

【０００３】第二のビジネスエンティティは、インターネットサービスプロバイダ（ISP）である。ISPは、そのサービスエリア内に一つあるいは複数のポイントオブプレゼンス（point of presence、POP）８を展開および管理し、エンドユーザはネットワークサービスを得るためにここに接続する。ISPは、ISPが顧客の加入を募る主要なローカルコーリングエリア内に、典型的には、一つのPOPを確立する。POPは、電話会社によって運用されるPSTNからのメッセージトラヒックを、ISPによって所有される、あるいはMCI, Inc.等のイントラネットバックボーンプロバイダからリースされるイントラネットバックボーン１０上で運ぶためのデジタル形式に変換する。ISPは、典型的には、PSTNへの接続のために、電話会社からT1ラインの一部もしくわ全部、あるいはT3ラインの一部もしくは全部をリースする。POPとISPのメディアデータセンタ１４は、イントラネットバックボーン上でルータ１２Ａを通じて互いに接続される。データセンタ１４は、IPSのウエブサーバ、メールサーバ、アカウンティングおよび登録サーバを収容し、ISPがウエブコンテント、ｅーメール、およびウエブホストサービスをエンドユーザに提供することを可能にする。将来の付加価値サービスは、データセンタ内に追加のタイプのサーバを展開することで追加することができる。ISPはさらにルータ１２Ａを公衆インターネットバックボーン２０への接続のために維持する。リモートアクセスに対する現在のモデルにおいては、エンドユーザはユーザの電話会社およびユーザのISPとの間にサービス関係を持ち、通常は両者から別個の請求書を受け取る。エンドユーザは、ISPにアクセスし、ISPから公衆インターネット２０にアクセスするが、これは最寄りのPOPにダイヤルし、インターネット技術標準化委員会（Internet Engineering Task Force、IETE）が勧告するポイトン・ツウ・ポイントプロトコル（point-to point protocol、PPP）として知られる通信プロトコルをランすることで行なう。

【０００４】第三のビジネスエンティティは、事業のために、自身のペライベートイントラネット１８を所有し、これをルータ１２Ｂを通じて運用する私企業である。企業の従業員は自宅あるいは路上から企業イントラネットネットワーク１８にアクセスすることができるが、これはPOTS/ISDN呼を企業のリモートアクセスサーバ１６にかけ、IETF PPPプロトコルをランすることで行なわれる。企業アクセスの場合は、エンドユーザは企業のリモートアクセスサーバ１６に接続するためのコストのみを支払う。この場合はISPは巻き込まれない。私企業は、エンドユーザを企業イントラネット１８、公衆インターネット２０、あるいは両方に接続するためにルータ１２Ｂを維持する。

【０００５】エンドユーザは、電話会社に、電話呼を発信するコストおよび電話回線を自宅に引くコストを支払う。エンドユーザは、さらにISPに、ISPのネットワークにアクセスすることおよびサービスに対してコトスを支払う。本発明は、無線サービスプロバイダ、例えば、Sprint PCS、PrimeCo等、並びに、インターネットサービスプロバイダ、例えば、AOL、AT&;T Worldnet等の両方にとって利益である。

【０００６】今日のインターネットサービスプロバイダは、ウエブコンテントサービス、ｅーメールサービス、コンテントホストサービスおよびローミングサービスをエンドユーザに提供する。マージンの低さや、特徴と価格に基づくマーケットセグメンテーションの展望のなさのために、ISPはマージンを向上するために付加価値サービスを求めている。短期的には、ISPは、設備ベンダによって提供される解決策を用いて、より迅速なアクセス、仮想プライベートネットワーキング（つまり、公衆ネットワークを用いて私設ネットワークと同程度に安全にイントラネットに接続する能力）、ローミングコンソーティアム、プッシュテクノロジー、およびサービス品質を提供することが見込まれる。長期的には、インターネット上での音声や、モビィリティも提供されることが見込まれる。ISPは、低マージンの激戦から脱却するために、これら付加価値サービスを用いることが見込まれる。ところで、これら付加価値サービスの内の多くは、ネットワークサービスの範疇に入るが、これらはネットワークインフラストラクチャ設備を通じてはじめて提供することが可能となる。他の幾つの付加価値サービスは、これもネットワークインフラストラクチャからのサポートを必要とするアプリケーションサービスの範疇に入り、他の幾つかはネットワークインフラストラクチャからのサポートは必要としない。迅速なアクセス、仮想プライベートネットワーキング、ローミング、モビィリティ、サービス品質、サービス品質に基づくアカウンティングは、全て、向上されたネットワークインフラストラクチャを必要とする。発明は、これら向上されたサービスを直接に提供するか、あるいは、将来さらに技術が進歩したときにこれらサービスを追加できるようにするためのフックを提供する。無線サービスプロバイダにとっては、収益奔流の大きなシェアを確保できることが見込まれ、ISPにとっては、より多くのサービス、より良好なマーケットセグメンテーションにて提供できることが見込まれる。

【０００７】

【発明の概要】本発明は、エンドユーザに、公衆インターネット、プライベートイントラネットおよびインターネットサービスプロバイダへのリモート無線アクセスを提供する。無線アクセスがフォーリンネットワーク内の基地局とホームネットワーク内の基地局を通じて両者のインターチエンジ合意の下で提供される。サービングインターワーキング機能と要求される通信サーバとの間の最適なルートが決定される。

【０００８】本発明の一つの目的は、モビィリティ管理

をローカル、マイクロ、マクロおよびグローバルの４つのコネクションハンドオーバのカテゴリに分割し、これらハンドオーバカテゴリに従ってハンドオフ更新を最小にするエンドユーザに対する無線パケット交換データネットワークを提供することにある。本発明のもう一つの目的は、MACハンドオフメッセージとネットワークハンドオフメッセージと統合することにある。本発明のさらにもう一つの目的は、別個に、登録機能は登録サーバに、ルーティング機能はインターワーキング機能ユニットに割り当てることにある。本発明のさらにもう一つの目的は、フォーリンネットワーク内の無線ハブ（アクセスハブAHとも呼ばれる）とインターワーキング機能ユニット（IWFユニット）との間に中間XTunnelチャネルを提供することにある。本発明のさらにもう一つの目的は、フォーリンネットワーク内のインターワーキング機能ユニットとホームネットワーク内のインターワーキング機能ユニットとの間にI-XTunnelチャネルを提供することにある。本発明のさらにもう一つの目的は、層２トンネリングプロトコル（layer two tinneling protocol、L2TP）をモバイルエンドシステムがサポートできるように強化することにある。本発明のさらにもう一つの目的は、PPP通信セッションの開始の前にネットワーク層の登録を遂行することにある。

【０００９】これらおよびその他の目的がホームネットワーク、フォーリンネットワークおよびエンドステーションを含むネットワーク内で達成される。フォーリンネットワークは、基地局およびサービング登録サーバを備えるフォーリンモバイル交換センタを含む。前記基地局は、サービングインターワーキング機能を備える無線ハブを含む。ホームネットワークは、ホーム登録サーバを備えるホームモバイル交換センタおよびホームインターワーキング機能を含む。エンドシステムはホームネットワークに加入し、フォーリンネットワーク内で動作する。エンドシステムは、登録リクエストを生成するためのエンドシステム登録エージェントを含む。この登録リクエストは、要求される通信サーバを持つ要求される通信ネットワークの指標を含む。エンドシステムは、登録リクエストをサービング登録サーバに送信する。サービング登録サーバは、第一のモジュールを含むが、これは登録リクエストを処理することで、要求される通信サーバと、ホームインターワーキング機能かサービングインターワーキング機能のいずれか一つとの間の最適なルートを決定する。サービング登録サーバは、さらに第二のモジュールを含むが、これは第一のモジュールが最適なルートがサービングインターワーキング機能と要求される通信サーバとの間であることを決定した場合、サービングインターワーキング機能を要求される通信サーバにリンクする。本発明を以下に、幾つかの好ましい実施例を図面を参照しながら詳細に説明することで詳細に説明する。

【００１０】

【発明の詳細な記述】本発明は、コンピュータユーザにインターネットやプライベートイントラネットへのリモートアクセスを仮想プライベーサネットワークサービスを用いて高速パケット交換無線データリンクを通じて提供する。これらユーザは、公衆インターネット、プライベートイントラネットあるいはユーザのインターネットサービスプロバイダに無線リンクを通じてアクセスすることができる。ネットワークは、ローミングをサポートする。ここで、ローミングとは、本発明によって提供されるサービスが利用可能な地域であればどこからでもインターネットやプライベートイントラネットに様々な仮想プライベートネットワークサービスを用いてアクセスできる能力を意味する。このネットワークは、さらに、ハンドオフをサポートする。ここで、ハンドオフとは、ユーザのネットワークへの接続ポイントを、PPPクライアントとPPPサーバとの間のPPPリンクとは透過的に変更できる能力を意味する。このネットワークは、水平インターネットやイントラネットアプリケーションをランしているユーザを対象にする。これらアプリケーションには、電子メール、ファイル転送、ブラウザベースのWWWアクセスや、インターネットの周辺に構築されるその他のビジネスアプリケーションが含まれる。このネットワークはIETF標準に準拠するために、このネットワーク上でRTP等のストリーミングメディアプロトコルやH.323等の会議プロトコルをランすることが可能である。

【００１１】既に展開済みあるいは展開の様々な段階にある他のインターネットリモートアクセス技術として、POTSおよびISDNに基づく有線ダイヤルアップアクセス、XDSLアクセス、GSM/CDMA/TDMAに基づく無線回路交換アクセス、ケーブルモデム、衛星ベースのシステム等が含まれる。ただし、本発明による方法は、低い展開コスト、容易な保守、広範な機能セット、スケーラビリティ、重負荷状況におけるグレースフルデグレーション等を特徴とすることに加え、仮想プライベートネットワークキング、ローミング、モビィリティ、ユーザとサービスプロバイダの相対的な利益のためのサービスの品質等の進歩したネットワークサービスをサポートする。

【００１２】パーソナル通信システム（PCS）のスペクトラムを所有する無線サービスプロバイダに対しては、本発明は、プロバイダがPSTNを所有および運用する従来の有線電話会社によって提供されるサービスと十分に競合できる無線パケット交換データアクセスサービスを提供することを可能となる。さらに、プロバイダは、インターネットサービスプロバイダとしても営業することを決意することもできる。この場合は、プロバイダは、ネットワーク全体を所有および運用し、エンド・ツウ・エンドサービスをユーザに提供することとなる。

【００１３】インターネットサービスプロバイダ（internet service providers、ISP）に対しては、本発明は

インターネ ットサービスプロバイダがこのスペクトラムを購入あるいはリースすることを前提に、電話会社をバイパスし、直接に、エンド・ツウ・エンドサービスをユーザに提供することができるようにする。この場合、将来インターネットの普及と共にますます上昇することが見込まれる電話会社へのアクセス料金が節約される。

【００１４】本発明はフレキシブルであり、このため、本発明は、インターネットサービスプロバイダ（ISP）ではなく、単に、エンドユーザに、ISP、インターネットあるいはプライベートイントラネットアクセスを提供する無線サービスプロバイダにとって有益であるばかりか、本発明はさらに、エンドユーザに無線アクセスおよびインターネットサービスを提供するサービスプロバイダにとっても有益である。本発明は、さらに、無線アクセスおよびインターネットサービスを提供するのみでなく、ネットワークの無線部分を他のISPあるいはプライベートイントラネットへのアクセスのために用いることを許すサービスプロバイダにとっても有益である。

【００１５】図２に示すように、エンドシステム３２（例えば、Win 95パーソナルコンピュータに基づく）は無線ネットワーク３０に外部あるいは内部モデムを用いて接続する。これらモデムは、エンドシステムがメディアアクセス制御（medium access control、MAC）フレームをエアリンク３４を通じて送受することを可能にする。外部モデムはＰＣに有線あるいは無線リンクを介して接続される。外部モデムは固定され、例えば、屋根上に搭載される指向性アンテナと同一位置に設置される。外部モデムは、ユーザのＰＣに、以下の手段：つまり、803.2、ユニバーサルシリアルバス、パラレルポート、赤外、さらには、ISM無線リンクの内の任意の一つを用いて接続することができる。内部モデムとしては、好ましくは、ラップトップに対するPCMCIAカードを用い、これがラップトップのバックプレーンに差し込まれる。これらは小型の全指向性アンテナを用いてMACフレームをエアリンク上を送受信する。

【００１６】エンドシステムは、加入者位置の所に設置される装置から成る。固定据付けの場合は、エンドシステムは、屋根に搭載されたアンテナ、無線要素、デジタル要素、およびデスクトップコンピュータから成る。加入者は既にデスクトップコンピュータを所有し、従って、この無線システムは、標準のインタフェースを通じてこのPCに接続されるものと想定する。図３～５は、無線システムの固定据付けに対する様々な典型的なオプションを示す。この図面に示される各オプションは、それぞれ、以下に説明する対応する据付けコスト、設備コスト、および据付け環境上の問題を持つ。

【００１７】図３に示す据付けは、現時点においては最も安価である。この構成においては、アンテナ２１のみが屋外に設置され、RFケーブル２２がラジオ２３に接続される。据付けを行なう者は、慣れた専門家であることも、加入者であることもあるが、アンテナ２１を、屋根か建物の側面に据付け、安価な延長ケーブル２２を建物に沿ってエントリポイントまで張る。これは、典型的には、窓枠の隅内の穴あるいは内側の床付近の壁内の穴を通して行なわれる。ラジオ２３は、デスクトップコンピュータ２４にとっては外部要素であり、これはPC２４にPCMCIAインタフェースを用いて接続する。ユーザがアクセスポイントから遠くに位置する場合は長いRFケーブルラン内の損失をインライン双方向RF増幅器によって補償する。ユーザがアクセスポイントに近接して位置する場合は、長いケーブルランの追加の損失は、これらの伝搬損失はセルの周辺の所のユーザほど大きくないために耐えることができる。

【００１８】図４に示すもう一つの設計においては、ラジオエレクトロニクスとアンテナが共通のデバイス２５に一体化される。PC２４への接続はベンダ独自のインタフェースおよびPCMCIAを用いて行なう。デバイスへの電力は壁変圧器２７から、電力とデジタルデータの両方を運ぶマルチツイステッドペアケーブル２６を介して供給する。このような一体化されたデバイスの設計には、防水、熱、冷却、サーバの高温および低温限度等を考慮することが必要となる。

【００１９】屋外アンテナと屋根裏部屋に搭載された加入者ユニットから成るもう一つの設計があり、この設計では低温と防水要件は解消されるが、ただし、この場合でも冷却は要求される。加入者ユニットは、ケーブルを介してPCに接続される。

【００２０】最後で最も高価なラジオからのデジタルデータを一つコンピュータあるいは複数のコンピュータに運ぶための手段は、図５に示すような、ISMバンドのLAN、例えば、WaveLANを用いる方法である。前述の取り据付け方法と同様に、アンテナ２１は屋根に設置され、ラジオはアンテナと同一箇所あるいは他の任意の箇所に設置される。802.3コネクションを用いてラジオを無線LANアクセスポイントに接続する。こうすることで、屋内の全てのリモートコンピュータデバイスが無線LAN２８へのアクセスを持つことになる。理想的には、無線LANアクセスポイントのアンテナ２９は、屋内のカバレッジを提供するとと同時に屋外へのRF漏れを最小にするために、建物の高所に、下向きに設置された指向性アンテナとされる。屋根裏部屋内にアンテナを設置した場合は、屋根裏部屋内でデバイスに電力を供給する問題や、LANラジオを冷却する問題等の様々な問題が発生する。実用上は、LANアンテナは、LANアクセスポイントに延びるアンテナケーブルの長さが短い限り、室内のどこに設置しても構わない。

【００２１】ラップトップコンピュータを自身のホームサービスエリア（ホームサービスエリア）から別のサービスエリアに持ち運ぶことを選択するローミング加入者にサービスを提供する必要性も存在する。この場合は、

ラップトップユーザは、アクセスポイントの方向を向くフラットパネル指向性アンテナを用いる必要がある。サービスポイントの整合は、サービス品質を確保するためには、非常に重要な要素となる。ラップトップソフトウエアとは別の整合インジケータを用いてアンテナを整合するためのガイドを得る。

【００２２】アンテナは、厚さは約１インチの１／２～３／４、開口はラットトップと概ね同一サイズ（８．５インチ×１１インチ）とされる。アンテナを持ち運ぶためには、アンテナパネルをラップトップに一時的に取り付けるための手段、例えば、フックとループファスナを用いると便利である。いったん、ラップトップユーザが、アクセスが要求される位置に到着したら、アンテナをラップトップの後部から取り出し、最良の性能が得られる方向に向ける。ただし、信号強度が非常に強いエリアではラップトップに取り付けたままでも構わない。さらに、ラップトップアンテナは、丁番にてラップトップに取り付け、二軸（バイアックス）整合機構を用いて、アンテナの方位角と仰角（上下左右）を調節することもできる。アンテナパネルは、４５°二重傾斜偏向をサポートするとともに、信号品質に影響を与える伝搬効果を除去するために、円錐ビーム形状を持つ。さらに、ビーム形状は、円錐形で二重偏向を持つために、アンテナはどちら側に立てても信号品質は変化しない。

【００２３】広いエリアの無線カバレッジが基地局３６によって提供される。基地局３６によって提供されるカバレッジのレンジは、リンク予算、容量およびカバレッジ等の様々な要因に依存する。基地局は、典型的には、セルサイト内にPSC（パーソナル通信サービス）無線サービスプロバイダによって設置される。基地局は、自身のカバレッジエリア内のエンドシステムから送られるトラヒックを多重化した上で有線回線あるいはマイクロ波バックホールネットワーク３８を通じてシステムのモバイル交換センタ（mobile switching center、MSC）４０に送信する。

【００２４】1997年12月26日付けでWalter Honcharenkoによって出願された“Multi-SectorCell Pattern For A Wireless Communication System”という名称の特許においては、マルチセクタ指向性アンテナ装置を備える無線通信システムが開示されているために、これも参照されたい。

【００２５】本発明は、エアリンクのMACとPHY（物理）層およびモデムのタイプに対しては独立である。本発明のアーキテクチャは、バックホールネットワーク３８の物理層およびトポロジに対しても独立である。バックホールネットワークに対する唯一の要件は、バックホールネットワークがインターネットプロトコル（IP）パケットを基地局とMSC（モバイル交換センタ）との間で十分な性能にてルーティングする能力を持つことである。モバイル交換センタ４０（MSC４０）においては、パケットデータインタワーキング機能（IWF）５２がこのネットワークに対する無線プロトコルを終端する。IPルータ４２はMSC４０を公衆インターネット４４、プライベートイントラネット４６あるいはインターネットサービスプロバイダ（ISP）４６に接続する。MSC４０内のアカウンティングおよびディレクトリサーバ４８はアカウンティングデータおよびディレクトリ情報を格納する。エレメント管理サーバ５０は、基地局、IWFおよびアカウンティング／ディレクトリサーバを含む装置を管理する。

【００２６】アカウンティングサーバは、アカウンティングデータをユーザに代わって収集し、このデータをサービスプロバイダの課金システムに送信する。アカウンティングサーバによってサポートされるインタフェースは、American Management Association（AMA）課金レコードフォーマットあるいは任意の他の適当な課金フォーマットにてのアカウンティング情報をTCP/IP（Transport control protocol/Internet protocol：トランスポート制御プロトコル／インターネットプロトコル）トランスポート層を通じて課金システム（これも図示せず）に送信する。

【００２７】ネットワークインフラストラクチャプロバイダは、PPP（point-to-point：ポイント・ツウ・ポイントプロトコル）サービスをエンドシステムに提供する。このネットワークは、エンドシステムに対して、（１）ローミングサービス（無線カバレッジが提供されている所ならどこでもログインできるサービス）付きの固定無線アクセス、および（２）低速モビィリティおよびハンドオフサービスを提供する。エンドシステムはネットワークにログオンしたとき、固定サービス（つまり、移動することなく、ハンドオフサービスを必要としないサービス）か、移動サービス（つまり、ハンドオフサービスを必要とするサービス）のいずれかをリクエストする。固定か移動かを指定しないエンドシステムは、移動サービスを指定したものとみなされる。エンドシステムの登録は、実際には、ホーム（オーム）登録サーバと協議して行なわれ、このとき、要求されるサービスのレベル、エンドシステムのユーザによって加入されるサービスのレベル、ネットワーク内の空いた設備等が考慮される。

【００２８】エンドシステムが協議の結果、固定サービス登録（つまり、ハンドサービスを必要としないサービス）を選択し、かつ、エンドシステムがホームネットワーク内に位置する場合は、IWF（インターワーキング機能）が基地局内に実現され、これによってトラヒックがエンドユーザと通信サーバ、例えば、PPPサーバ（つまり、接続されるべきポイント、例えば、ISP PPPサーバ、企業イントラネットPPPサーバ、あるいは無線サービスプロバイダによって顧客に公衆インターネットへの直接のアクセスを提供するために運用されるPPPサーバ等）との間で中継される。メッセージトラヒックの約８

０％がこのカテゴリに入ることが見込まれる。つまり、このアーキテクチャは、IWF処理を基地局に分散させることで中央モバイル交換センタ内でメッセージトラヒックが輻湊するのを回避する。

【００２９】他方、エンドシステムが（ホームネットワークあるいはフォーリンネットワークからの）移動サービスをリクエストした場合、あるいは、エンドシステムがローミングサービス（つまり、ホームネットワークからフォーリンネットワークに移動するサービス）を要求した場合は、サービングIWFとホームIWFとの２つのIWFが確立される。サービングIWFは、典型的には、エンドシステムが接続したネットワーク（これはホームネットワークであるかフォーリンネットワークであるかは関係ない）の基地局内に確立され、ホームIWFは、典型的には、ホームネットワークのモバイル交換センタ（MSC）内に確立される。この状況は、メッセージトラヒックの約２０％を占めるのみであるものと見込まれるために、モバイル交換センタにおけるメッセージトラヒックの輻湊は最小限にとどまる。サービングIWFと無線ハブは、コンピュータの同一ネスト内に同一位置に配置あるいは同一のコンピュータ内にプログラムされるために、トンルネルを無線ハブとサービングIWFとの間にXTunnelプロトコルを用いて設定する必要はない。

【００３０】ただし、別の方法として、フォーリンネットワーク内のサービングIWFは、利用可能な設備と要求されるサービスのタイプや品質に基づいて、フォーリンMSC内の設備から選択することもできる。一般的には、ホームIWFがアンカーポイントとなり、これは通信セッションの際に変更されることはなく、サービングIWFの方はエンドシステムが大きく移動すると変更される。

【００３１】基地局は、アクセスハブと少なくとも一つのアクセスポイントを含む（アクセスポイントは、アクセスハブと離して設置することも、同一位置に設置することもできる）。アクセスハブは、典型的には、複数のアクセスポイントを扱う。エンドシステムはアクセスポイントに有線あるいはケーブルによって接続することもできるが、ただし、本発明の一つの好ましい実施例においては、エンドシステムは、アクセスポイントに無線“エアリンク（air link）”によって接続され、この場合、アクセスハブは便宜的に無線ハブと呼ばれる。ここでの説明では、アクセスハブは全般に渡って“無線ハブ（wireless hub）”として示される。ただし、エンドシステムをアクセスポイントを通じてアクセスハブに有線あるいはケーブルを介して接続することも可能であり、この場合は“アクセスハブ（accesshub）”という用語が用いられる。

【００３２】本発明においては、エンドシステムは、エンドユーザ登録エージェント（例えば、エンドシステムのコンピュータ、そのモデム、あるいは両方の上でランするソフトウエア）を含み、これはアクセスポイントと通信、あるいはアクセスポイントを通じて、無線ハブと通信する。無線ハブは、代理（プロキシ）登録エージェント（例えば、無線ハブ内のプロセッサ上でランするソフトウエア）を含み、これはエンドユーザ登録エージェントに対する代理として機能する。この代理登録エージェントと類似する概念が、例えば、IETFによって提唱されるMobile IP標準においては、通常、フォーリンエージェント（foreing agent、FA）と呼ばれている。このため、本発明による代理登録エージェントは、以降、フォーリンエージェントと呼ぶことにし、以下の説明においては、本発明のフォーリンエージェントがIETFによって提唱されるMobile IP標準のフォーリンエージェントと異なる場合にのみの説明する。

【００３３】基地局内に代理登録エージェント（つまり、フォーリンエージェント（FA））を用いることで、エンドシステムのユーザ登録エージェントは、ネットワークへの接続のポイントを見つけ、ホームネットワークのMSC（モバイル交換センタ）内の登録サーバに登録することが可能になる。ホーム登録サーバは、ネットワーク内の複数のインターワーキング機能（IWF）モジュール（実際にはMSCおよび無線ハブの両方の中に設置されたプロセッサ上でランするソフトウエアモジュール）の空き状況を決定し、IWFを登録されたエンドシステムに割り当てる。登録された各エンドシステムに対して、基地局内の無線ハブとモバイル交換センタ（MSC）内のインターワーキング機能（IWF）との間にトンネルが（XTunnelプロトコルを用いて）設定され、このトンネルによって、PPPフレームがエンドシステムとIWFとの間で輸送される。

【００３４】ここで用いられるXTunnelプロトコルとは、PPPデータフレームのシーケンシャルな輸送を提供するフロー制御を備えたプロトコルを意味する。このプロトコルは、標準のIPネットワーク上、ポイント・ツウ・ポイントネットワーク上、あるいはATMデータネットワークやフレームリレーデータネットワーク等の交換式のネットワーク上でランする。これらネットワークは、T1あるいはT3リンクに基づくことも、無線リンクに基づくことも考えられ、さらに、地上ベースであることも、空中ベースであることも考えられる。XTunnelプロトコルは、L2TP（level 2transport protocol）からのアルゴリズムを適応化することによって構築することができる。ただし、データパケットの損失を伴うリンクに基づくネットワークの場合は、再送機能が必須のオプションとなる。

【００３５】エンドシステムのPPPピア（つまり、通信サーバ）は、IWF内あるいは企業イントラネットもしくはISPのネットワーク内に駐在する。PPPピアがIWF内に駐在する場合は、エンドシステムには、直接インターネットアクセスが提供される。PPPピアがイントラネットもしくはISP内に駐在する場合は、エンドシステムに

は、イントラネットアへのクセスもしくはISPへのアクセスが提供される。イントラネットあるいはISPアクセスをサポートするためには、IWFは、層２トンネルプロトコル（L2TP）を用いて、イントラネットあるいはISPのPPPサーバに接続する。イントラネットあるいはISPのPPPサーバの視点からは、IWFは、ネットワークアクセスサーバ（network access server、NAS）のように見える。エンドシステムとIWFとの間のPPPトラヒックは基地局内のフォーリンエージェントによって中継される。

【００３６】逆（登りリンク）方向の場合は、エンドシステムからIWFに向かうPPPフレームは、MACおよびエアリンクを通じて、基地局に送られる。基地局は、これらフレームを、MSC内のIWFにXTunnelプロトコルを用いて中継する。IWFは処理のためにこれらをPPPサーバに配達する。インターネットアクセスの場合は、PPPサーバは、IWFと同一のマシン内に位置する。ISPあるいはイントラネットアクセスの場合は、PPPサーバはプライベートネットワーク内に位置し、IWFは層２トンネルプロトコル（L2TP）を用いてこれに接続する。

【００３７】順（下りリンク）方向の場合は、PPPサーバからのPPPフレームは、IWFによって基地局にXTunnelプロトコルを用いて中継される。基地局は下りリンクフレームをトンネルから取り出し（デトンネルし）、これをエアリンクを通じてエンドシステムに中継する。次にこのフレームはエンドシステムのPPP層によって処理される。

【００３８】モビィリティ（移動性）をサポートするために、ハンドオフに対するサポートが含まれる。MAC層は基地局およびエンドシステム内のモビィリティ管理ソフトウエアがハンドオフを効率的に遂行することを支援する。ハンドオフはピアPPPエンティティおよびL2TPトンネルからは透過的に扱われる。エンドシステムが一つの基地局から別の基地局に移動すると、新たなXTunnelが新たな基地局と当初のIWFとの間に生成される。以前の基地局からの以前のXTunnelは削除される。PPPフレームはこの新たな経路を用いて透過的に運ばれる。

【００３９】ネットワークは、ローミング機能（つまり、エンドユーザがフォーリン無線サービスプロバイダを通じて自身のホーム無線サービスプロバイダに接続する機能）をサポートする。この機能を用いると、エンドシステムは、ホームネットワークから離れてフォーリンネットワークにローミングした場合でもサービスを受けることができる。勿論、これは、フォーリン無線サービスプロバイダとエンドシステムのホーム無線サービスプロバイダとがサービス合意を持つことを前提とする。

【００４０】図６は、ローミングエンドシステム６０がフォーリン無線サービスプロバイダ６２がカバレッジを提供する位置まで旅行（ローミング）した状況を示す。ただし、これは、ローミングエンドシステム６０がホーム無線サービスプロバイダ７０と加入者関係を持つことを想定する。さらに、本発明においては、ホーム無線サービスプロバイダ７０がフォーリン無線サービスプロバイダ６２とアクセスサービスを提供する契約関係を持つことを想定する。こうして、図示するように、ローミングエンドシステム６０は、フォーリン無線サービスプロバイダ６２の基地局６４にエアリンクを通じて接続する。次に、データがローミングエンドシステム６０からフォーリン無線サービスプロバイダ６２の基地局６４およびサービングIWF６６を通じてホーム無線サービスプロバイダ７０のホームIWF７２に中継され、場合によっては、さらに、ホーム無線サービスプロバイダ７０のホームIWFを通じてインターネットサービスプロバイダ７４に中継される。

【００４１】ローミングをサポートするためには、I-インタフェースと呼ばれるサービスプロバイダ間インタフェースが無線サービスプロバイダ（wireless service provider、WSP）の境界間の通信のために用いられる。このインタフェースは、認証のため、登録のため、およびエンドシステムのPPPフレームをフォーリンWSPとホームWSPとの間で輸送するために用いられる。

【００４２】PPPフレームは、登りリンク方向と下りリンク方向の両方において、エンドシステムのホーム無線サービスプロバイダ（WSP）を通じて運ばれる。ただし。別の方法として、PPPフレームをフォーリンWSPから直接に宛先ネットワークに輸送するこもとできる。フォーリンWSP内の基地局はフォーリンネットワークにおけるエンドシステムの接続のポイントである。このフォーリンWSP内の基地局は、PPPフレームをフォーリンWSPのモバイル交換センタ内のサービングIWFに送信、あるいはサービングIWFからPPPフレームを受信する。サービングIWFは、I-インタフェースを通じて、層２トンネルを用いて、ホームIWFと接続し、エンドシステムのPPPフレームを双方向に輸送する。フォーリンWSP内のサービングIWFは監査ためにアカウンティングデータを収集し、ホームWSP内のホームIWFは課金のためにアカウンティングデータを収集する。フォーリンWSP内のサービングIWFは同一システム内の基地局と結合し、これによってX-Tunnelの必要性を排除することもできる。

【００４３】登録フェーズの際に、フォーリンWSP内の登録サーバはローミングエンドシステムのホームネットワークの識別を調べる（決定する）。フォーリン登録サーバはこの情報を用いてホーム登録サーバと通信し、エンドシステムの認証および登録を行なう。これら登録メッセージはＩ－インタフェースを用いて輸送される。エンドシステムの認証および登録が成功すると、一つの層２トンネルが、基地局とサービングIWFの間にXTUNNELプロトコルを用いて生成され、もう一つの層２トンネルが、サービングIWFとホームIWFの間にＩ－インタフェースを通じて生成される。ホームIWFはエンドシステムのPPPピアに前と同様にL2TP（level 2 tunnelprotocol）を

用いて接続する。ハンドオフの際は、ホームIWFの位置とこのL2TPトンネルは固定されたままにとどまる。エンドシステムが一つの基地局からもう一つの基地局に移動すると、新たなトンネルが、新たな基地局とサービングIWFとの間に生成され、以前の基地局とサービングIWFとの間の以前のトンネルは削除される。エンドシステムがさらに遠くまで移動し、新たなサービングIWFが必要になった場合は、新たなトンネルが、新たなサービングIWFとホームIWFとの間に生成され、以前のサービングIWFとホームIWFとの間の以前のトンネルは削除される。

【００４４】ローミングをサポートするために、Ｉ－インタフェースは、認証サービス、登録サービス、および無線サービスプロバイダの境界間でデータを輸送するサービスをサポートする。認証サービスと登録サービスは、IETF Radiusプロトコルを用いてサポートされる。PPPフレームを層２トンネルを通じて輸送するデータ輸送サービスは、I-TXunnelプロトコルを用いてサポートされる。このプロトコルは、IETF L2TPプロトコルに基づく。

【００４５】ここでの説明に用いられるホームIWFという用語は、エンドシステムのホームネットワーク内のIWFを指し、サービングIWFという用語は、フォーリンネットワーク内のエンドシステムに一時的にサービスを提供しているIWFを指す。同様に、ホーム登録サーバという用語は、エンドシステムのホームネットワーク内の登録サーバを指し、フォーリン登録サーバという用語は、エンドシステムがローミングしている最中にそれを通じて登録を行なうフォーリンネットワーク内の登録サーバを指す。

【００４６】ネットワークは、エンドシステムに対して、固定と動的の両方のIPアドレス割り当てをサポートする。考慮すべき２つのタイプのIPアドレスが存在する。第一のアドレスは、エンドシステムの自身のホームネットワーク内の識別である。これは、user@domainなるフォーマットを持つ構造化されたユーザ名である。これは、mobile IPにおいて用いられるホームIPアドレスとは異なる。第二のアドレスは、エンドシステムにPPP IPCアドレスプロトコルを介して割り当てられるIPアドレスである。ホームアドレスのドメインサブ欄（domain sub-field）は、ユーザのホームドメインを識別するために用いられ、完全修飾ドメイン名である。ホームアドレスのユーザサブ欄（user sub-field）は、ユーザをホームドメイン内で識別するために用いられる。User-Nameがエンドシステム上と、MSCの所の加入者データベース内に格納され、これは、ユーザにユーザがサービスに加入する際に割り当てられる。User-Nameのドメインサブ欄はローミングの際に登録および認証の目的で、ローミング関係とホーム登録サーバを識別するために用いられる。この構造化されたユーザ名の代わりに、他の一意の識別子を用いてユーザのホームネットワークおよびユーザをホームネットワーク内で識別することもできる。この識別子は、エンドシステムによって登録リクエストに挿入して送られる。

【００４７】PPP IP Configuration Protocol（PPP IPコンフィギュレーションプロトコル）がエンドシステムに対してIPアドレスを協議するために用いられる。IP Configuration Protocol（IPCP）を用いることで、エンドシステムは、固定か動的のいずれかのIPアドレスを協議することができる。

【００４８】上述のように、ホームアドレスは使用せず、代わりに構造化されたUser-Name欄を使用する方法は、本発明が周知のIPと異なる一つの特徴である。ただし、本発明のネットワークは、将来モバイルIPとこれのPPPエンドシステムとの関連での使用がもっと一般化した場合は、User-Name欄は持たず、非零のホームアドレスのみを持つエンドシステムもサポートできるように改良することが考えられる。この場合、サービスプロバイダによって、IPCPアドレス割り当てフェーズの際にエンドシステムのホームアドレスと同一のIPアドレスを割り当てるPPPサーバを構成することが考えられる。この場合、ホームアドレスとIPCPによって割り当てられるIPアドレスとは同一となる。

【００４９】図７に示すように、基地局６４とエンドシステムからのエアリンクによって無線サブネットワーク８０が形成され、この無線サブネットワーク８０は、エンドユーザアクセスのためのエアリンク、少なくとも一つの基地局（例えば、基地局６４）、および基地局からMSC４０（図２）に向かう少なくとも一つのバックホールネットワーク（例えば、図２の３８）を含む。例えば、３セクタから成る基地局の無線サブネットワークアーキテクチャは、以下の論理機能を含む。

【００５０】１．アクセスポイント機能（Acess point function）。アクセスポイント８２は、MAC層ブリッジング、並びに、MAC層のアソシエーションとディソシエーション手続きを遂行する。アクセスポイントは、プロセッサ（好ましくは顧客アプリケーションに特化された集積回路（ASIC）の形式）、無線ハブへのリンク（好ましくはカード上のイーサネットリンクあるいはASIC内に組み込まれた形式）、アンテナへのリンク（好ましくはデータ変／復調器と送／受信機を備えるカードの形式）およびアンテナを含み、このアンテナにエンドシステムが結合される。プロセッサは、後に詳細に説明する登録およびモビィリティハンドオーバをサポートするデータブリッジング機能および他の様々な機能を遂行するソフトウエアをランする。これら機能については、後の図１０、１１、１４の説明の部分を参照されたい。

【００５１】アクセスポイント（AP）は、エアリンクからMAC層のフレームを受け取り、これらを無線ハブに送信、あるいは逆に無線ハブからのフレームをエアリンク（エンドシステム）に送信する。MAC層のアソシエーシ

ョンとディソシエーション手続きは、APによって、エンドシステムのMACアドレスのリストを自身のMACアドレスフィルタテーブル内に維持するために用いられる。APは、エンドシステムに代わってMAC層ブリッジングを遂行するが、このとき、MACアドレスが自身のMACアドレスフィルタテーブル内に存在するエンドシステムのみが扱われる。アクセスポイントと、それと関連する無線ハブは、典型的には、同一位置に配置される。アクセスポイントは、最も単純な形式においては、単に無線ハブへのポートの形式を取る。APと無線ハブが同一のセルサイト内に同一位置に置かれる場合、これらは、IEEE 802.3リンクを介して互いに接続される。しばしば、アクセスポイントは、無線ハブから離して置かれ、有線T1等のトランク長距離リンクや、場合によっては無線トランクを介して接続される。複数のセクタから成るマルチセクタセルの場合、複数のアクセスポイントが用いられ、各セクタに１つが割り当てられる。

【００５２】２．無線ハブ機能（Wireless hub function）。無線ハブ８４は、フォーリンエージェント（FA）手続き、バックホール負荷のバランシング（例えば複数のT1を使用）、バックホールネットワークインタフェーシング、およびxtunnel手続きを遂行する。サービス品質（QOS）に対するサポートがなされている場合は、無線ハブは、異なるQOS属性を持つバックホールネットワーク上でxtunnelプロトコルをランすることによって、QOSに対するサポートを実現する。複数のセクタから成るマルチセルサイトの場合は、典型的には、単一の無線ハブ機能が複数のアクセスポイントによって共有される。無線ハブは、プロセッサ、一つのあるいは複数のアクセスポイントへのリンク（好ましくはカード上のイーサネットリンクあるいはASIC内に組み込まれた形式）、およびバックホール回線へのリンクを含む。バックホール回線は、典型的には、T1あるいはT3通信回線であり、無線サービスプロバイダのモバイル交換センタに終端する。バックホール回線へのリンクは、データを、イーサネットフォーマット、フレームリレーフォーマット、あるいはATMフォーマット等の好ましいフォーマットにフォーマット化する。無線ハブプロセッサは、後に詳細に説明するデータブリッジングおよび他の様々な機能をサポートするソフトウエアをランする。これに関しては、後の図１２、１３、１４の説明の部分を参照されたい。基地局の設計は、以下のタイプのセルアーキテクチャをサポートする。

【００５３】１．ローカルAPアーキテクチャ（Local AP architecture）。ローカルAPアーキテクチャの場合は、アクセスポイントは大きな（典型的には２ｋｍ以上）のレンジを持つ。これらは、セルサイト内に、無線ハブと同一位置に配置される（図４）。アクセスポイントは、無線ハブにIEEE 802.3ネットワークを用いて接続することも、無線ハブのバックプレーン内に直接に差し込むことも、あるいは無線ハブに幾つかの他の機構（例えば、ユニバーサルシリアルバス、プリンタポート、赤外線等）を用いて接続することも考えられる。ここでの説明の残りの部分では、第一の代替を用いるものと想定する。セルサイトはオモニ形式にすることも、無線ハブに複数のアクセスポイントとセクタ化されたアンテナを加えることでセクタ化することもできる。

【００５４】２．リモートAPアーキテクチャ（Remote AP architecture）。リモートAPアーキテクチャの場合は、アクセスポイントは、通常は、非常に小さなレンジ、典型的には、半径約１ｋｍのレンジを持つ。これらは、無線ハブから離れて（室内あるいは屋外に）配置される。リモートアクセスポイントは、好ましくは、T1あるいは無線トランクを用いて、無線ハブが位置するセルサイトにリンクされる。セルサイトからは、典型的には、有線のバックホール回線あるいはマイクロ波リンクを用いて、MSC内のIWFに接続される。リモートAPと無線ハブとの間に無線トランキングが用いられる場合は、トランキングに対してオムニ（全指向性）あるいはセクタ化された無線ラジオが利用される。リモートアクセスポイントへのトランキングのためのデバイスは、好ましくは、無線ハブと同一位置に配置し、これにIEEE 802.3ネットワークを用いて接続するか、あるいは、直接に無線ハブのバックプレーンに差し込む。これらトランキングのためのデバイスは、以降、トランクAPと呼ばれる。

【００５５】３．混合型APアーキテクチャ（Mixed AP architecture）。混合型APアーキテクチャの場合は、無線サブネットワークは、リモートおよびローカルアクセスポイントをサポートする必要がある。ホールフィリングや、他の容量上の理由により複数のリモートアクセスポイントを追加することも考えられる。前述のように、リモートAPは無線ハブにT1あるいは無線トランクを用いて接続される。

【００５６】図３７および３８は可能な接続を示すシステム構成図である。ケース（１）の場合は、IWF１がアンカーIWFであり、ホームエージェントとして機能し、他方、WH１はフォーリンエージェントとして機能する。WH１とIWF１との間にはXtunnelが用いられ、IWF１とPPPサーバとの間にはlayer 2 Tunneling protocol（L2TP）トンネルが用いられる。ケース（２）の場合は、WHとサービングIWF２は、同一位置に設置される。IWF１がアンカーIWFであり、サービングIWF、つまり、IWF２が、Foreign agent（フォーリンエージェントとして機能する。IWF１とIWF２との間にはI-Xtunnelが用いられ、IWF１とPPPサーバとの間にはL2TPトンネルが用いられる。ケース（３）の場合は、サービングIWFはIWF３であり、アンカーIWFはIWF１である。WH３とIWF３との間にはXtunnelが用いられ、IWF３とIWF１の間にはI-Xtunnelが用いられ、IWF１とPPPサーバとの間にはL2TPトンネルが用いられる。

【００５７】図３８は、無線ホップ（トランクAP）の追加を示す。ここで、トランクAPは、WHと同一位置に配置することもできる。この場合は、上述の３つの可能性の全てに加えて、以下の可能性も考えられる。ケース（１）の場合は、トランクAP１がフォーリンエージェントであり、IWF１がアンカーIWFである。トランクAP１とアンカーIWFとの間にはXtunnelが用いられ、アンカーIWFとPPPサーバとの間にはL2TPトンネルが用いられる。ケース（２）の場合は、サービングIWF２がフォーリンエージェントである。トランクAP２とIWF２との間にはXtunnelが用いられ、IWF２とアンカーIWF１との間にはI-Xtunnelが用いられ、アンカーIWFとPPPサーバとの間にはL2TPトンネルが用いられる。ケース（３）の場合は、サービングIWFがフォーリンエージェントである。トランクAP３とIWF３との間にはXtunnelが用いられ、IWF３とアンカーIWF１との間にはI-Xtunnelが用いられ、アンカーIWF１とPPPサーバとの間にはL2TPトンネルが用いられる。

【００５８】図３９～４２は、幾つかのハンドオフシナリオおよびシステムの要素間の様々な接続を示す。図８は、ローカルAPのみを用いる３つのセクタを持つセルを示す。アクセスポイントと無線ハブは基地局内に同一位置に配置され、互いに802.3リンクを用いて接続される。図９は、リモートアクセスポイント８２が無線ハブ８４に無線トランク８６を用いて接続されるアーキテクチャを示す。基地局内の各トランクアクセスポイント８６は、リモートマイクロアクセスポイント８２（図面ではR-AP）へのポイント・ツウ・マルチポイント無線ラジオリンクを提供する。リモートアクセスポイントは、エンドシステムに対してエアリンクサービスを提供する。無線ハブとトランクアクセスポイントは基地局内に同一位置に配置され、802.3リンクを介して互いに接続される。この図面には、さらに、ポイント・ツウ・ポイントT1リンクを介して無線ハブに接続されるリモートアクセスポイント８２Ｒも示される。後者のシナリオではトランクAPは必要とされない。

【００５９】上述の全てのセルアーキテクチャ、および各セルによって用いられることが考えられる全ての異なるタイプのアクセスポイントをサポートするためにネットワークアーキテクチャは以下の規則に従う：

【００６０】１．アクセスポイントはMAC層ブリッジとして機能する。リモートアクセスポイントは、エンドシステムへのエアリンクとセルサイトへの無線あるいはT1トランクとの間のMACブリッジングを遂行する。ローカルアクセスポイントは、エンドシステムへのエアリンクと無線ハブとの間のMACブリッジングを遂行する。

２．トランクアクセスポイントもMAC層ブリッジとして機能する。これらはトランク（これはアクセスポイントに向かう）と無線ハブとの間のMACブリッジングを遂行する。

３．無線ハブは全ての同一位置に配置されたMACブリッジ（つまり、ローカルアクセスポイントあるいはトランクアクセスポイント）に最初は802.3リンクを用いて接続する。

【００６１】加えて、T1トランクを備えるローカルアクセスポイントあるいはリモートアクセスポイントが用いられる場合は、以下の規則に従う：

１．ローカルアクセスポイントは、無線ハブと同一位置に配置し、これにポイント・ツウ・ポイント802.3リンクあるいは共有802.3ネットワークを用いて接続する。リモートアクセスポイントは無線ハブにポイント・ツウ・ポイントT1トランクを用いて接続される。

２．セクタ化は、セルサイトにアクセスポイントをセクタ化されたアンテナと共に追加することでサポートする。

３．無線アクセスポイントに接続された各アクセスポイントに対して、その無線ハブ内で実行するフォーリンエージェントが存在する。MAC層アソシエーション手続きを用いて、アクセスポイントのMACアドレスフィルタテーブルが最新の状態に維持され、MAC層ブリッジングが効率的に遂行される。無線ハブがMACアソシエーション機能に参加し、このため正当なMACアドレスのみがアクセスポイントのMACアドレスフィルタテーブルに加えられる。

【００６２】４．IWFが無線ハブと同一位置に位置しない限り、無線ハブは、アクセスポイントからのフレームをMSC IWFに向けてあるいはこの逆にxtunnelプロトコルを用いて中継する。MACアドレスフィルタテーブルを用いて、そのMACアドレスがテーブル内に存在しないユニカーストMACデータフレームが除去される。APは、MACブロードキャストフレームとエンドシステムの登録機能と関係するMACフレームについてはMACアドレスフィルタテーブルの内容と関係なく常に中継する。

５．ローカルアクセスポイントはIPトラヒックを無線ハブにルーティングするためにARPを用いてMACアドレスを解決する。逆方向において、無線ハブもARPを用いてIPパケットをアクセスポイントにルートする。アクセスポイントのネットワーク管理のためにUDP/IPを用いる。

【００６３】６．T1を介して接続されたリモートアクセスポイントは、このリンクはポイント・ツウ・ポイントリンクであるためにARPは用いない。

７．ハンドオフに対するサポートはMAC層からの支援の下で行なわれる。

【００６４】無線トランクとトランクAPを用いるセルアーキテクチャでは以下の規則に従う：

１．トランクアクセスポイントは、無線ハブと同一位置に配置され、これにポイント・ツウ・ポイント802.3リンクあるいは他の適当な手段を用いて接続される。

２．無線トランクのセクタ化はセルサイトにトランクアクセスポイントをセクタ化されたアンテナと共に追加す

ることでサポートする。
３．バックホールセクタ間のハンドオフは、無線ハブ内のフォーリンエージェントを用いて行う。各バックホールセクタに対して、無線ハブ内で実行するフォーリンエージェントが存在する。
【００６５】４．トランクAPは、MAC層におけるエンドシステムのアソシエーションとハンドオフ手続きに参与する必要はない。これらのMACアドレスフィルタテーブルは、エンドシステムがネットワークに登録すると無線ハブによって動的にプログラムされる。MACアドレスフィルタテーブルを用いてユニカーストMACフレームが除去される。ブロードキャストMACフレームあるいは登録パケットを含むMACフレームについては常に通過することが許される。
【００６６】５．トランクAPは、IPトラヒックを無線ハブにルーティングするためにARPを用いてMACアドレスの解決を行なう。反対方向においては、無線ハブはARPを用いてIPパケッ トをトランクAPにルートする。UDP/IPがトランクAPのネットワーク管理に用いられる。
６．単一無線トランクセクタにおいては、MACアソシエーションと、あるアクセスポイントから別のアクセスポイントへのハンドオフは、MAC層を無線ハブ内のフォーリンエージェントの支援の下で用いて行なう。これらMAC層手続きを用いてエンドシステムがアクセスポイントと関連付けられる。エンドシステムが一つのアクセスポイントから別のアクセスポイントに移動すると、アクセスポイントはMACハンドオフプロトコルを用いて自身のMACアドレスフィルタテーブルを更新する。セルサイトの所の無線ハブが、アクセスポイントがこの機能を遂行する際の支援を提供する。この支援には、MAC層ハンドオフメッセージの中継（これはアクセスポイントは直接にMAC層を通じて互いに通信することはできないためである）、MAC層登録およびハンドオフに対するエンドシステムの認証、およびアクセスポイントのMACアドレスフィルタテーブルの更新が含まれる。
【００６７】７．無線トランクセクタに対するフォーリンエージェントがフレームをそのトランクAPからMSCにあるいはこの逆方向にxtunnelプロトコルを用いて中継する責任を持つ。このため、トランクAPに対するフォーリンエージェントは、その無線トランクセクタ内でのエンドシステムのアクセスポイントに関しての位置は感知しない。下りリンク方向においては、このフォーリンエージェントは、単に、モバイルIPトンネルからのフレームを適当なトランクAPに転送するのみであり、このトランクAPがMAC層ブリッジングを用いてこれらフレームをそのバックホールセクタに接続された全てのリモートアクセスポイントに送信する。次に、これらリモートアクセスポイントが自身のMACアドレスフィルタテーブルを調べ、結果に基づいて、そのMACフレームをアクセスネットワーク上に転送、あるいはMACフレームを脱落させる。上述のように、MACアドレスフィルタテーブルはMAC層アソシエーションとハンドオフ手続きを用いて最新の状態に維持される。登り方向においては、MACフレームはリモートアクセスポイントによってバックホールブリッジに転送され、バックホールブリッジがこれらを無線ハブ内のフォーリンエージェントに802.3リンクを用いて転送する。
【００６８】８．IPパケットをリモートアクセスポイントに送信あるいはこれから受信するためにARPは用いない。リモートアクセスポイントは無線ハブのMACアドレスをBOOTP手続きを用いて決定する。逆に、無線ハブはリモートアクセスポイントのMACアドレスを用いて構成される。アクセスポイントのネットワークネットワーク管理、およびエンドシステムのアソシエーションとハンドオフメッセージにはUDP/IPを用いる。セルサイト内のIEEE 802.3リンクはより高速のリンクと交換することもできる。
【００６９】図１０は、ローカルアクセスポイントのプロトコルスタックを示す。このスタックのベースには物理層PHYが存在する。物理層PHYは、データをエンドシステムとの間で、空中、例えば、無線波を用いて送受信する。これらデータはストリームにてデータ変調器に送信あるいは復調器から受信される。APがエンドシステムからのデータを物理層を通じて受信した場合は、APは、これをMACフレーム（MAC層）にアンパックする。次に、このMACフレームは、イーサネット物理層フォーマット（IEEE 802.3フォーマット）に再パックされ、イーサネットリンクを介して無線ハブに送信される。逆に、APのプロセッサがエンドシステムに伝送されるべきデータを無線ハブからイーサネットリンク（つまり、物理リンク）を介して受信した場合は、APは、そのデータをメディアアクセス制御（MAC）フォーマットにパックし、次に、このMAC層データを変調器に送信する。次に、変調器がこのデータをエンドシステムにPHY層を用いて送信する。
【００７０】図１１においては、図１０に示すエンドシステムに向かう／あるいはこれからのMAC層とPHY層が、セルサイトへのトランクに対するリモートアクセスポイントのMAC層とPHY層と置換される。T1トランク上では、好ましくは、ハイレベルデータリンクプロトコル（high level data link protocol、HDLCプロトコル）を用いる。
【００７１】図１２は、バックホール回線とエンドアクセスポイントへのトランクをブリッジする無線ハブのプロトコルスタックを示す。リモートAPへのトランクはリモートアクセスポイントのサポートのみに要求される（これとは対照的にイーサネットはアクセスポイントを接続する）。リモートAPへの無線トランクのMAC層とPHY層は、ポイント・ツウ・マルチポイントリンクを提供し、一つのトランクが同一セクタ内の複数のリモートAP

と通信するために用いられる。

【００７２】無線ハブはリモートAPへのトランクとネットワークのモバイル交換センタ（MSC）へのバックホール回線（例えば、T1あるいはT3）をブリッジする。無線ハブ内のプロトコルスタックは、MSCへのMAC層とPHY層を実現し、この上部にはIP（Internet Protocol）層が実現され、さらにこの上部にはネットワーク管理のためのUDP（Universal Datagram Protocol）層が実現され（IP層とUDP層は組み合わせてUDP/IPと呼ばれる）、さらにこの上部にはXTunnelプロトコルが実現される。XTunnelプロトコルは新たなフォーマットであり、これは、モビィリティ（例えば、mobile IPにおけるモビィリティ）の特徴と、Level 2 Tunnel Protocol（L2TP）の特徴の両方を備える。XTunnelプロトコルは、無線ハブからMSCへの通信、および、異なるネットワークあるいは同一ネットワーク内のインターワーキング機能（IWF）間の通信のために用いられる。

【００７３】図１３はリモートアクセスポイントをサポートするための基地局内のリレー機能のプロトコルスタックを示す。このリレー機能には、バックホール回線へのインタフェース（無線ハブとして示す）とリモートAPへのインタフェース（トランクAPとして示す）が含まれる。無線ハブの観点からは、（図１３に示す）トランクAPは、実際には、図１０に示すAPのように振る舞う。好ましくは、基地局のプロトコルスタックは、無線ハブとトランクAPに分割され、この間をイーサネットによって接続される。Ｎ個のセクタから成る無線トランクの場合は、セルサイト内のＮ個の無線トランクAPと１個の無線ハブが存在する。

【００７４】図１４はローカルAPを用いるセルアーキテクチャの基地局のプロトコルスタックを示す。リレー機能には、バックホール回線へのインタフェース（無線ハブとして示す）とエンドシステムへのエアリンクインタフェース（APとして示す）が含まれる。無線ハブの観点からは、（図１１、１４に示す）APは、実際には図１１に示すトランクAPのように振る舞う。好ましくは、基地局のプロトコルスタックは、無線ハブとトランクAPとの分割され、これらがイーサネットによって接続される。Ｎ個のセクタから成るセルの場合は、Ｎ個のアクセスポイントと１個の無線ハブが存在する。

【００７５】基地局からMSCへのバックホールネットワークは以下の属性を持つ：

１．このネットワークはIPデータグラムを基地局とMSCとの間でルーティングする能力を持つ。

２．このネットワークはセキュリティである。これは、公衆インターネットではない。このネットワークはエンドシステムのトラヒックを輸送するためのみでなく、認証、アカウンティング、登録、および管理トラヒックも輸送するために、信託された（トラストされた）ノードからのトラヒックのみがこのネットワーク上に入ることを許される。

３．このネットワークは必要な性能特性を備える。

４．基地局は、IP over Ethernetリンクをサポートする。典型的なアプリケーションにおいてはサービスプロバイダはその上に装置を設置するバックホールネットワークを設置および維持する責任を持つ。

【００７６】基地局はMSCと通信するために、以下のバックホールインタフェースをサポートする：

１．基地局は、IP over PPP with HDLC link（IETF標準）をポイント・ツウ・ポイントT1リンクあるいはT3リンクの一部分を用いてサポートる。

２．基地局は、IP over frame relay（IETF標準）をT1リンクあるいはT3リンクの一部分を用いてサポートする。

３．基地局は、IP over AAL5/ATM（IETF標準）をT1リンクあるいはT3リンクの一部分を用いてサポートする。

【００７７】上述のインタフェースは全てIETF標準のカプセル化に基づくため、MSC内に市販のルータを用いてこのバックホールネットワークの物理リンクを終端することができる。より上位の層は、様々なサーバや他のプロセッサにパスされ、そこで処理される。MAC層の上部のエンドシステム登録手続きがサポートされる。以下の説明ではMAC層の所のエンドシステム登録手続きは、上位の層に影響を与えない限り無視される。

【００７８】エンドシステムはサービスを求めてホームネットワークからあるいはフォーリンネットワークから登録する。両方のシナリオにおいて、エンドシステムは基地局内のフォーリンエージェント（FA）を用いて、登録のためのネットワークへの接続ポイントを見つける。前者の場合、FAはエンドシステムのホームネットワーク内に存在し、後者の場合、FAはフォーリンネットワーク内に存在する。いずれの場合も、ネットワークはエンドシステムのホームネットワーク内のIWFをアンカーポイント（つまり、移動してもセッションを通じて変更されないポイント）として用いる。エンドシステムへのあるいはこれからのPPPフレームは、基地局内のFAを介してホームネットワーク内のIWFに送られる。エンドシステムがホームにいる場合は、ホームIWFは直接にxtunnelプロトコルを介して基地局に接続される。ホームIWFは、基地局と同一ノードに結合することもできることに注意する。エンドシステムがフォーリンにローミングしている場合は、フォーリンネットワーク内のサービングIWFはホームIWFにＩ－インタフェースを用いて接続される。サービングIWFもまた基地局と同一ノードにて結合できることに注意する。サービングIWFは基地局とホームIWFとの間でフレームを中継する。ホームIWFからは、データは、同一のIWF内に駐在するPPPサーバに送られることも、別個のサーバにL2TPを用いて送られることもある。別個のサーバは無線サービスプロバイダとは異なるプライベートネットワークオペレータ（例えば、ISPあ

るいは企業イントラネット）によって所有および運用される。このセッションの最中、ホームIWFとPPPサーバの位置は固定されたままにとどまる。エンドシステムが接続した状態で移動した場合、これは、新たなフォーリンエージェントに再登録することが必要となる。ただし、同一のIWFとPPPサーバが引き続いて用いられる。新たなFAとIWFとの間に新たなxtunnelが生成され、以前のフォーリンエージェントとIFWとの間の以前のxtunnelは削除される。

【００７９】図１５は、２つのエンドシステムＡ、Ｂに対するこのネットワークの第一の構成（コンフィギュレーション）を示す。ここでは、これらエンドシステムの両方のホーム無線ネットワークは無線サービスプロバイダＡ（WSP-A）である。一方のエンドシステムはホーム無線ネットワークから登録し、他方のエンドシステムはフォーリン無線ネットワークから登録する。WSP-A内のホームIWFが両方のエンドシステムに対するアンカーポイントとして機能する。両方のエンドシステムについて、データはホームIWFに中継される。ホームIWFはISP-Aによって所有されるインターネットサービスプロバイダのPPPに接続する。ここでは、両方のエンドシステムが同一のISPに加入しているものと想定する。ただし、別のISPに加入している場合は、ホームIWFは別のISPにも接続される。

【００８０】無線サービスプロバイダのネットワーク内部においては、基地局とIWFの間ではデータはxtunnelプロトコルを用いて運ばれる。IWFとPPPサーバの間ではデータはLevel 2 Tunneling Protocol（L2TP）を用いて運ばれる。サービングIWFとホームIWFとの間では、データはI-xtunnelプロトコルを用いて運ばれる。

【００８１】単純なシナリオにおいては、固定サービスを要求する自身のホームネットワーク内のユーザに対しては、ホームIWF機能は、基地局内で動的に起動することもできる。また、サービングIWF機能は、基地局内のローミングユーザに対して起動することもできる。常にホームネットワーク内のIWFを用いることには長所と短所がある。最も明らかな長所は単純なことである。短所は、常に、リモートのホームIWFとの間でデータを中継することが必要になることである。代替として、サービングIWFによってエンドシステムのISP／イントラネットに接続するために必要とされる全ての情報をサービングIWFに送信し、サービングIWFがアカウンティング情報をリアルタイムにてホームネットワーク内のアカウンティングサーバに送り返す方法も考えられる。この機能は実現はより困難であるが、データをフォーリンネットワークからホームネットワークに長距離に渡って中継する必要性が低減されるために効率は良くなる。

【００８２】例えば、シカゴから香港にローミングするユーザのケースについて考える。ユーザのホームネットワークがシカゴに存在し、ユーザが香港内の無線サービスプロバイダを用いて登録するものと想定する。この場合、第一の構成では、アンカーポイントはシカゴ内のホームIWFとなり、全てのデータを香港とシカゴり間で中継することが必要となる。シカゴ内のホームIWFはシカゴ内のユーザのIPSに接続する。これに対して第二の構成では、エンドシステムのユーザには香港内のISPが割り当てられる。このために、データをシカゴと香港の間で常に中継する必要はなくなる。第二の構成では、サービングIWFがアンカーとして機能し、サービングIWFはエンドシステムが移動した場合でもセッションを通じて変更されない。ただし、FAの位置はエンドシステムが香港内で移動すると変更される。

【００８３】図１６は、第二のネットワーク構成を示す。この図面では、エンドシステムＡ、Ｂに対するホームネットワークはWSP-Aである。エンドシステムＡは、ホームネットワークから登録し、ホームIWFをアンカーポイントとして用い、また、ISP-AにISPのPPPサーバを用いて接続する。エンドシステムＢの方は、WSP-Bのフォーリンネットワークから登録し、サービングIWFを用いる。このサービングIWFは、アンカーポイントとして機能するとともに、エンドシステムをISPにISPのPPPサーバを用いて接続する。この構成では、エンドシステムＢのデータはフォーリンネットワークとホームネットワークの間を中継する必要はなくなる。

【００８４】この構成が機能するためには、ホームとフォーリンの無線サービスプロバイダの間にローミング合意があるのみでなく、フォーリン無線サービスプロバイダとエンドシステムのインターネットサービスプロバイダとの間にも、直接にあるいは仲介者を通じて、合意があることが必要となる。上述の例では、香港内の無線サービスプロバイダとシカゴ内の無線サービスプロバイダがビジネス合意を持つことに加えて、香港内のWSPが、エンドシステム（ユーザ）のChcago ISPとの間に、香港内のChcago ISPのPPPサーバにアクセスすることに関するビジネス合意を持つか、あるいは、ユーザのChcago ISPとの間にローミングに関するビジネス合意を持つ香港内に位置する他のISPとの間にビジネス合意を持つことを要求される。加えて、香港内のWSPは、ユーザの認証、アカウンティング、適当なトンネルの設定等を遂行するためにこれらのローミング関係を動的に発見できることを要求される。

【００８５】インターネットインフラストラクチャ事業に従事する様々な企業が、IETF（インターネット技術標準化委員会）において、適当な基準をこれら全てのシナリオに対して策定するまでには、まだ時間がかかると思われる。このため、現時点では、前者のより単純なホームネットワーク内のIWFが常にアンカー点として用いられる構成が、多少効率は落ちるが、本発明の好ましい実施例とされる。ただし、インターネットローミングに対するプロトコルの適当な産業標準が策定された暁には第

この構成についても同等なあるいは代替の実施例として考慮されるべきである。

【００８６】エンドシステムは、PPPを開始しデータを送受するためには、その前に、無線ネットワークに登録する必要がある。このため、エンドシステムは、最初に、FAの発見と登録のフェーズに入る。これらフェーズを通じてエンドシステムが認証され、無線サービスプロバイダに登録される。これらフェーズが終了すると、エンドシステムはPPPを開始する。これには、PPPリンク設定フェーズ、PPP認証フェーズ、およびPPPネットワーク制御プロトコルフェーズが含まれる。いったんこれらフェーズが終了すると、エンドシステムはPPPを用いてIPパケットを送受することが可能になる。

【００８７】以下の説明においては、エンドシステムがフォーリンにローミングしており、フォーリンネットワークから登録するものと想定する。FA発見フェーズにおいて、エンドシステムは（自身のユーザ登録エージェントを通じて）フォーリンエージェントからのアドバタイズメントを要請する。ユーザ登録エージェントは付近のフォーリンエージェントによって送信されたアドバタイズメントメッセージ（advertisement messages）を用いて、登録のためのFAの識別を見つる。この登録フェーズにおいて、エンドシステムのユーザ登録エージェントは、FAを選択し、それに向けて登録リクエストを発行する。FAは、代理（プロキシ）登録エージェントとして機能し、この登録リクエストをフォーリン登録サーバ（フォーリンWSP内の登録サーバ）に転送する。フォーリン登録サーバは、ユーザ登録エージェントのリクエスト内のUser-Name欄を用いて、エンドシステムのホームネットワークを調べ、この登録リクエストを、認証のために、ホームネットワーク内の登録サーバに転送する。ホーム登録サーバはフォーリン登録サーバによって中継された登録リクエストを受信すると、フォーリン登録サーバの識別とエンドシステムの識別の認証を行なう。認証と登録が成功すると、ホーム登録サーバはホームネットワーク内のIWFを選択し、ホームIWFと（フォーリンWSP内の）サービングIWFとの間にI-xtunnelリンクを生成する。ホームネットワーク内のIWFは、このPPPセッションを通じて終始アンカー点として機能する。

【００８８】いったんモービルIP（mobile IP）の認証および登録フェーズが終了すると、様々なPPPフェーズが開始される。PPPの開始時に、ホームIWFと要求されたISP／イントラネットPPPサーバとの間にL2TP接続が生成される。PPP認証フェーズにおいては、PPPパスワードがPAPあるいはCHAPを用いて交換され、ISPあるいはイントラネットPPPサーバは独自にエンドシステムの識別の認証を行なう。

【００８９】いったんこれが成功すると、PPPネットワーク制御フェーズが開始される。このフェーズにおいては、IPアドレスが協議され、IPアドレスがPPPサーバによってエンドシステムに割り当てられ、TCP/IP見出しの圧縮の使用についても協議される。これが終了すると、エンドシステムは、自身のISPあるいは企業イントラネットとの間でIPパケットをPPPを用いて送受することが可能になる。

【００９０】認証が２つのレベルで遂行されることに注意する。モービルIPの認証においては、エンドシステムの識別がホームネットワーク内のホーム登録サーバと比較され、さらに、フォーリンネットワークの識別とホームネットワークの識別が互いに比較される。この機能を遂行するために、フォーリンエージェントは、エンドシステムの登録リクエストを、例えば、IETE Radiusプロトコルを用いて自身のローカルMSC内のフォーリン登録サーバにRadius Aceess-Requestパケットに入れて送信する。フォーリン登録サーバはエンドシステムのドメイン名を用いてエンドシステムのホームネットワークとホーム登録サーバの識別を決定し、Radius代理として機能することで、このリクエストをカプセル化し、エンドシステムのホーム登録サーバに転送する。一方、フォーリン登録サーバがエンドシステムのホームネットワークの識別を決定できない場合は、フォーリン登録サーバは、オプションとして、Radiusリクエストを、ブローカのように機能する登録サーバ（例えば、無線サービスプロバイダの協会によって所有される登録サーバ）に転送することもできる。この場合は、このブローカが代わって、Radius Aceess-Requestを最終的なホーム登録サーバに送る。このローカル登録サーバが、その登録リクエストをローカル的にあるいは代理として扱うことができない場合は、ローカル登録サーバはそのフォーリンエージェントの登録リクエストを拒絶し、次に、フォーリンエージェントがエンドシステムの登録リクエストを拒絶する。他方、ホーム登録サーバは、Radius Access-Requestを受信すると、フォーリンネットワークとエンドシステムの識別について必要な認証を遂行する。認証と登録が成功すると、ホーム登録サーバは、Radius Access-Responseパケットをフォーリン登録サーバに送り返し、次に、フォーリン登録サーバが応答をフォーリンエージェントに送り、こうして、ラウンドトリップ（一巡）が完了する。登録リクエストは、ホームサーバがなんらかの理由で受諾しない場合は拒絶される。

【００９１】第二のレベルに認証動作においては、エンドシステムの識別がイントラネットあるいはISPのPPPサーバと比較される。モビリティ認証とは別個にPPP認証を行なうことで、インフラストラクチャ設備をISPとは別個に展開および所有するこが可能になる。

【００９２】図１７は、ローミングエンドシステムに対する登録シーケンスを示す梯子図である。PPPサーバとホームIWFは同一サーバ内に位置し、L2TPは必要ないものと想定する。登録エンドシステムに代わってアカウンティングを開始するために行なわれるアカウンティング

サーバとの対話、並びにホーム登録サーバの識別を決定するためおよびエンドシステムの識別を認証するためのディレクトリサーバとの対話についても示される。ただし、アカウンティング、課金、（サービスプロバイダ間の）ローミング、および清算に関しては後に説明する。

【００９３】エンドシステムのユーザ登録エージェントからのMAC層メッセージ（例えば、802.11ビーコン）によって、Agent Solicitationが開始される。MAC層のメッセージは、図面を簡潔化するために示されていない。

【００９４】図１７に示すように、最初に、エンドシステム（モバイル）がアドバタイズメントを要請し、フォーリンエージェントがアドバタイズメントを送り返す。エンドシステムは、このアドバタイズメントからフォーリンエージェントが属するネットワークに関する情報を知る。この情報には、フォーリンエージェントの気付けアドレスも含まれる。別の方法として、このフェーズは、削除し、全てのネットワークアドバタイズメントを絶えず放出されるMAC層のビーコンメッセージによって遂行することもできる。ここでの説明においては、このネットワークはフォーリン無線サービスプロバイダであるものと想定する。次に、エンドシステム内のユーザ登録エージェントが、フォーリンエージェントとそのネットワークに関する情報（気付けアドレスも含め）を登録リクエストに組み入れ、この登録リクエストをフォーリンエージェントに送る。このフォーリンエージェントは、代理（プロキシ）登録エージェントとして機能し、登録リクエストをフォーリン登録サーバ（つまり、フォーリン無線サービスプロバイダの登録サーバ）に中継する。すると、フォーリン登録サーバは、そのリクエストがホームディレクトリではないことを認識し、フォーリンディレクトリサーバにアクセスする。フォーリンディレクトリサーバはフォーリン無線サービスプロバイダのFDD（フォーリンドメインディレクトリ）を用いて、その登録リクエストをエンドシステムが属する無線サービスプロバイダのホーム登録サーバにどのようにして送信すれば良いか調べ、次に、この転送のために必要な情報をフォーリン登録サーバに送り返す。次に、フォーリン登録サーバは、エンドシステムの登録リクエストをRadiusアクセスリクエスト内にカプセル化し（組み入れ）、このカプセル化したリクエストを、そのエンドシステムが属する無線サービスプロバイダのホーム登録サーバに中継する。すると、ホーム登録サーバはホームディレクトリサーバにアクセスし、ホームディレクトリサーバは、ホーム登録サーバのHDDを用いて少なくともフォーリンサービスプロバイダについての認証情報を調べ、これをホーム登録サーバに送り返す。オプションとして、ホーム登録サーバは、加入者のディレクトリにアクセスすることで、詳細な加入者サービスプロフィル情報（例えば、加入しているサービスオプションの品質等）を得ることもできる。結果として、全てのパーティが認証されると、ホーム登録サーバはホームIWFとPPPサーバにstart IWF request（IWF開始リクエスト）を送信する。ホームIWFとPPPサーバはホームアカウンティングサーバを始動し、その後、start IWF response（開始確認応答）をホーム登録サーバに送り返す。すると、ホーム登録サーバは、Radius access response（Radiusアクセス確認応答）をフォーリン登録サーバに送る。次に、フォーリン登録サーバは、start IWF request（IWF開始リクエスト）をサービングIWFに送る。サービングIWFは、サービングアカウンティングサーバを始動し、その後、start IWF response（開始確認応答）をフォーリン登録サーバに送り返す。フォーリン登録サーバは登録応答をフォーリンエージェントに送り、フォーリンエージェントはこの登録応答をエンドシステムに中継する。

【００９５】次に、エンドシステムが、リンク制御プロトコル（link control protocol、LCP）コンフィギュレーションリクエストを、フォーリン登録サーバを通じて、ホームIWFとPPPサーバに送る。すると、ホームIWFとPPPサーバは、LCPコンフィギュレーション確認応答を、フォーリン登録サーバを通じて、エンドシステムに送り返す。

【００９６】次に、エンドシステムは、同様に、パスワード認証プロトコル（password authentication protocol、PAP）認証リクエストをホームIWFとPPPサーバに送り、ホームIWFとPPPサーバは、PAP確認応答をエンドシステムに返す。別の方法として、認証のためにchallenge authentication protocol（CHAP）（認証挑戦プロトコル）を用いることもできる。認証のために両方のプロトコルを用いることも、このフェーズはスキップすることもできる。

【００９７】次に、エンドシステムは、同様に、IPコンフィギュレーションプロトコル（IPconfiguration protocol、IPCP）をホームIWFとPPPサーバに送り、ホームIWFとPPPサーバはPCP確認応答を送り返す。

【００９８】エンドシステムへの接続は以下の理由の任意の一つによって終端される。

１．ユーザ始動の終端。このシナリオの下では、エンドシステムが最初にPPPをグレースフルに終端させる。これには、PPPネットワーク制御プロトコル（IPCP）の終端と、これに続く、PPPリンクプロトコルの終端が含まれる。いったんこれが行なわれると、エンドシステムのネットワークへの登録が解除され、続いて、アクセスポイントへの無線リンクが終端される。

２．無線リンクの損失。このシナリオはエンドシステム内のモデムによって検出され、モデムドライバに報告される。すると、ソフトウエアの上位層にスタックを終端する通告が送られ、終端がユーザに通知される。

【００９９】３．フォーリンエージェントへの接続の損失。このシナリオは、エンドシステム内のモビリティドライバによって検出される。（潜在的に新たな）フォ

ーリンエージェントとコンタクトすることを再び試み、失敗した場合は、ドライバは、適当な通知を上位のプロトコルスタックに送り、同時に、下位のモデムに信号を送り、無線リンクを終端させる。

４．IWFへの接続の損失。これは、フォーリンエージェントへの接続が失われた場合と実質的に同一である。

５．IWFあるいはPPPサーバによるPPPの終端。このシナリオは、エンドシステム内のPPPソフトウエアによって検出され、エンドシステムのPPPドライバにこの事象が通知される。PPPドライバは、ネットワークへの登録の解除を試み、続いて、アクセスポイントへの無線リンクを終端する。

【０１００】エンドシステムのサービスコンフィギュレーションとは、ネットワークサービスをエンドシステムに対して加入者のサービスプロフィルに基づいて構成する概念を意味する。加入者のサービスプロフィルは、加入者ディレクトリ内に格納されている。ソフトウエアは、このサービスプロフィルに含まれる情報を用いて、無線データサービスを加入者に代わってカスタム化する。この情報には、エンドシステムの認証、エンドシステムのローミング、エンドシステムのインターネットサービスプロバイダへの接続の設定等に用いる情報が含まれる。この情報には、さらに、好ましくは、サービスの品質等の他のパラメータも含まれる。加入者ディレクトリに加え、ホームドメインディレクトリ（HDD）とフォーリンドメインディレクトリ（FDD）がローミングおよびフォーリン登録サーバとホーム登録サーバを互いに認証するために用いられる。HDDは、エンドシステムのホームネットワークに関する情報を格納し、FDDは、加入者が訪問するフォーリンネットワークに関する情報を格納する。

【０１０１】図１８は、これらディレクトリがいかにネットワークアーキテクチャにマッピングされ、これらがホームから登録するエンドシステムに対して登録の際にいかに用いられるかを示す。ステップ０において、エンドシステム（モバイル）がアドバタイズメントを要請し、フォーリンエージェントがアドバタイズメントを介してエンドシステムにそのフォーリンエージェントが属するネットワークに関する情報を供給する。このケースにおいては、このネットワークはホーム無線サービスプロバイダであるものと想定される。ステップ１において、エンドシステム内のユーザ登録エージェントが、こうして得られたフォーリンエージェントとそのネットワークに関する情報をリクエスト内に組み入れ、このリクエストをフォーリンエージェントに送信する。ステップ２において、フォーリンエージェントが、代理登録エージェントとして、このリクエストをホーム登録サーバに中継する。ステップ３において、ホーム登録サーバが、ホーム無線サービスプロバイダのHDDにアクセスすることで、少なくとも認証情報を得る。ステップ４において、ホーム登録サーバは、さらに、加入者ディレクトリにアクセスすることで、詳細な加入者サービスプロフィル情報（例えば、加入されるサービスオプションの品質等）を得る。ステップ５において、ホーム登録サーバがフォーリンエージェントにアクセス確認応答を送り返す。ステップ６と７において、フォーリンエージェントがエンドシステム（つまり、モバイル）に登録の確認応答を送り返す。

【０１０２】図１９は、フォーリンネットワークから登録するエンドシステムに対するディレクトリの使用を示す。ステップ０において、エンドシステム（モバイル）がアドバタイズメントを要請し、フォーリンエージェントがアドバタイズメントを介して、エンドシステムに、そのフォーリンエージェントが属するネットワークに関する情報を供給する。このケースにおいては、このネットワークは、フォーリン無線サービスプロバイダであるものと想定される。ステップ１において、（エンドシステム内の）ユーザ登録エージェントは、フォーリンエージェントとそのネットワークおよびそのセキュリティ証明（セキュリティクレデンシャル）に関する情報をリクエスト内に組み入れ、このリクエストをフォーリンエージェントに送信する。ステップ２において、フォーリンエージェントが、代理登録エージェントとして、このリクエストをフォーリン登録サーバ（つまり、フォーリン無線サービスプロバイダの登録サーバ）に中継する。ステップ３において、フォーリン登録サーバがフォーリン無線サービスプロバイダのHDDにアクセスすることで、エンドシステムが属するネットワークの情報を得る。ステップ４において、フォーリン登録サーバが、エンドシステムのリクエストを、エンドシステムのホーム無線サービスプロバイダのホーム登録サーバに転送する。ステップ５において、ホーム登録サーバがホーム登録サーバのFDDにアクセスし、少なくともフォーリンサービスプロバイダに関する認証情報を得る。ステップ６において、ホーム登録サーバは、さらに、加入者のディレクトリにアクセスすることで、詳細な加入者サービスプロフィル情報（例えば、加入するサービスオプションの品質等）を得る。ステップ７において、ホーム登録サーバがフォーリン登録サーバに、アクセス確認応答を送り返す。ステップ８において、フォーリン登録サーバがフォーリンエージェントにアクセス確認応答を転送する。ステップ９において、フォーリンエージェントがエンドシステム（つまり、モバイル）に登録確認応答を送り返す。

【０１０３】以下では、ベアラデータを扱うプロトコルハンドリングのシナリオおよびベアラデータをエンドシステムとの間の送受するための関連するスタックを、ローカルAPを用いるセルアーキテクチャ（図２０）と、リモートAPを用いるセルアーキテクチャ（図２１）に対する両方のプロトコルスタックについて説明する。

【０１０４】図２０は、ホームネットワーク内のエンドシステムとホームIWFとの間の通信を扱うためのプロトコルスタックをEnd System@Homeに対して示す。図２０は、アクセスポイントと無線ハブが同一位置に配置される場合のセルアーキテクチャに対するプロトコルハンドリングを示す。図２１は、アクセスポイントと無線ハブが離して配置される場合のセルアーキテクチャに対するプロトコルハンドリングを示す。図示するようにPPPはIWF内に終端し、この構成は直接インターネットアクセスを提供する。PPPサーバとIWFが離されるケースの構成については後に説明する。

【０１０５】図２１に示すように、エンドシステムからのPPPフレームはRLP（radio link protocol）フレーム内にカプセル化され、これらはさらにリモートアクセスポイントの所でMACフレーム内にカプセル化され、トランクアクセスポイントに送信される。トランクアクセスポイントは、無線ハブと物理的に接近して位置するアクセスポイントであり、リモートアクセスポイントはトランクアクセスポイントに、一例として、無線トランクによって接続される。このリモートアクセスポイントは、MAC層ブリッジとして機能し、エアリンクからのフレームを無線ハブ内のフォーリンエージェントに中継する。フォーリンエージェントは、MACフレームからRLPフレームを取り出し、このRLPフレームをxtunnelプロトコルを用いてIWFに中継する。IWFからエンドシステムに送られるフレームの場合も方向が逆であることを除いて類似するプロセスが発生する。

【０１０６】エンドシステムが別のフォーリンエージェントに移動すると、新たなフォーリンエージェ ントとIWFとの間に新たなxtunnelが自動的に生成され、PPPトラヒックはこれらの間を中断されることなく運ばれる。リモートAPとトランクAPとの間に無線トランクを用いるリモートAPセルアーキテクチャでは（図２１）、エンドシステムとアクセスポイントとの間のエアリンクは、トランクの無線技術および周波数（ｆ２）とは異なる無線技術および周波数（ｆ１）を用いて動作する。

【０１０７】図２２は、ローミングエンドシステムに対するプロトコルスタックを示す。サービングIWFは、サービングIWFとホームIWFとの間にI-xtunnelプロトコルを用いる。プロトコルスタックの他の部分は、上述と同一であるため特に示さない。このアーキテクチャは、サービングIWFを基地局内に併合し、XWDプロトコルを除去することで単純化することもできる。

【０１０８】RLP層は、シーケンス番号を用いることで、重複するPPPデータグラムを脱落させ、エンドシステムとIWFとの間でPPPデータグラムをシーケンスに配信する。RLP層は、さらに、エンドシステムとIWFとの間のリンク接続性を監視するためにコンフィギァラブルキープアライブ機構を用いる。代替の実施例においては、RLP層は、さらに、エンドシステムとIWFとの間のリンクの総ビットエラー率を低減するために再送およびフロー制御サービスを提供する。エンドシステムとIWFの間のRLPはセッションの開始時に始動され、セッションを通じてハンドオフの間もアクティブにとどまる。

【０１０９】mobile IP RFC（RFC 2003）の仕様とは対照的にフォーリンエージェントとホームIWFとの間のトンネリングにIP in IP encapsulationは用いられない。この代わりに新たなトンネリングプロトコルがUDPの上に実現される。この新たなトンネリングプロトコルはL2TPプロトコルを簡素化したバージョンである。新たなこのトンネリングプロトコルを用いる理由は以下の通りである：

【０１１０】１．RFC 2003において規定されるカプセル化プロトコルでは、フロー制御、すなわちパケットのシーケンス配信は提供しない。ただし、本発明のネットワークはバックホールを通じてのトンネル内でこのサービスをエアリンクの上の再送の量を低減するために必要とする。つまり、フロー制御を用いることで、基地局とMSCとの間のネットワーク上のフロー制御問題に起因するパケット損失や、基地局あるいはIWF内のフロー制御問題に起因するパケット損失が低減される。

【０１１１】２．このトンネリングプロトコルはUDPベーであるため、ユーザレベルにて実現し、性能を保証するためのデバッグの後にカーネルに入れることができる。

３．RFC 2003を用いた場合、サービス品質と負荷バランスを考慮に入れてトンネリングを生成するのは簡単ではない。QOSを考慮に入れるためには、既に要求されるQOSを提供するリンク上にトンネルを設定できる必要がある。第二に、RFC2003を用いた場合は、基地局とMSCとの間の複数のリンクの間にベアラトラヒックを分散させ、負荷をバランスさせるのは簡単ではない。

【０１１２】４．RFC 2003において規定されるようにIP in IP encapsulationを実現するためには、開発者はIPソースコードへのアクセスが必要となる。商用のオペレーティングシステムの場合、TCP/IPスタックに対するソースコードは、通常、別個の商品（所有プログラム）として開発されており、他のベンダとの互換性がない。ベンダからTCP/IPスタックを購入し、mobile IP tunnelingをサポートするたにIP層に変更を加える場合、開発業者はTCP/IPスタックの様々なバージョンを絶えずサポートすることを要求される。これには追加のコストとリスクが伴う。

【０１１３】本発明による基地局とIWFとの間のトンネリングプロトコルは非標準であり、無線サービスプロバイダは異なるベンダからの装置を混合し、整合させることはできない。ただし、非標準のトンネリングプロトコルを単一の無線サービスプロバイダのネットワーク内で用いた場合、これは、エンドシステムや他のベンダからの装置には透過的であることに注意する。

【０１１４】この新たなトンネリングプロトコルはL2TPに基づく。L2TP自体は、重いトンネリングプロトコルであり、L2TPはトンネルの生成および認証と関連する大きなオーバーヘッドを持つ。L2TPと比べ、本発明による新たなトンネリングプロトコルはオーバヘッドが小さい。この新たなxtunnelおよびI-Xtunnelプロトコルは、以下の特徴を持つ：

１．このxtunnelおよびI-Xtunnelの生成は、基地局と登録サーバとの間で用いられるRadius Access Request（Radiusアクセス要求）と、Radius Access Response（Radiusアクセス応答）メッセージにベンダ固有の拡張を追加する。これら拡張はトンネルパラメータを協議し、トンネルを生成する。

【０１１５】２．登録サーバは、パケットをトンネリングおよび中継する実際の仕事は様々な異なるIPアドレス、従って、MSC内の異なるサーバに委託することができる。このため、登録サーバは、複数のIWFサーバ間で負荷のバランスを取ること、および様々なユーザに異なるQOSを提供することが可能になる。

【０１１６】３．このxtunnelおよびI-Xtunnelプロトコルは、トンネル管理に対する帯域内制御メッセージをサポートする。これら制御メッセージとしては、トンネルの接続性をテストするためのエコーリクエスト／応答、トンネルを切断するための切断リクエスト／応答／通知、およびエラーを通知するためのエラー通知が含まれる。これらメッセージは、UDP/IP等のトンネリング媒体上を送信される。

【０１１７】４．このxtunnelおよびI-Xtunnelプロトコルは、ペイロードデータをUDP/IP等のトンネリング媒体上に送信する。このxtunnelおよびI-Xtunnelプロトコルは、フロー制御とパケットのシーケンス配信をサポートする。

５．このxtunnelおよびI-Xtunnelプロトコルは、サービス品質を確保する目的でUDP/IP以外の媒体上に実現することもできる。

【０１１８】本発明によるネットワークは、直接インターネット接続性をサポートする。これは、PPP をホームIWF内に終端し、このIWFからのIPパケットをルータを介して標準のIPルーティング技術を用いてインターネットにルーティングすることで達成される。好ましくは、IWFとルータは両方ともRIPをランするが、場合によっては、OSPF等の他のルーティングプロトコルをランすることもできる。

【０１１９】このネットワークは、同時にインターネットサービスプロバイダでもある無線サービスプロバイダ（WSP）に対して第一の構成をサポートする。この構成においては、MSC内のホームIWFはPPPサーバとしても機能する。このホームIWFもRIP等のインターネットルーティングプロトコルをランし、インターネットサービスプロバイダのバックボーンネットワークへの接続するためにルータを用いる。

【０１２０】このネットワークは、WSP自身はインターネットサービスプロバイダ（ISP）ではないため、あるいはそのWSPがエンドユーザにアクセスを提供する合意を他のISPとの間でにもつために、エンドシステムを一つあるいは複数のインターネットサービスプロバイダに接続することを希望する無線サービスプロバイダに対して第二のコンフィギュレーションをサポートする。例えば、ある無線サービスプロバイダ（WSP）がエンドユーザにネットワークアクセスを提供することを選択し、さらに、第三者であるISPとの間に、その第三のISPとも取引のあるエンドユーザが、そのWSPネットワークからその第三のISPにアクセスするのを許す合意を持つ状況がこれに相当する。この構成においては、PPPサーバは、MSCの所に設置されるホームIWF内ではランしない。代わりに、L2TP（Layer Two Tunneling Protocol）等のトンネリングプロトコルを用いてISPのPPPサーバにトンネルバックする。図１０はこの構成に対するプロトコルスタックをホームに位置するエンドシステムに対して示す。

【０１２１】ホームIWFとISPのPPPサーバの位置は、PPPセッションを通じて固定されたままにとどまる。ホームIWFとISPのPPPサーバとの間のL2TPトンネルもPPPセッションを通じて設定されたままにとどまる。ホームIWFとPPPサーバとの間の物理リンクはルータを介して専用のT1もしくはT3、あるいはフレームリレーもしくはATMネットワークを用いて設定される。この物理リンクの個々の特性はこのアーキテクチャの観点からは特に重要ではない。

【０１２２】この構成は、イントラネットアクセスもサポートする。イントラネットアクセスの場合は、PPPサーバは企業イントラネット内に駐在し、ホームIWFはL2TPを用いてこれにトンネリングする。

【０１２３】図２３は、イントラネットあるいはISPアクセスに対するプロトコルハンドリングを固定エンドシステムに対して示す。これは、上述の構成とローミングエンドシステムは自身のホームIWFに接続するためにサービングIWFを用いる点が異なる。サービングIWFとホームIWFとの間のプロトコルハンドリングは前述の通りである。図２３において、ホームIWFを無線ハブ内に併合することで、X-tunnelプロトコルを除去することもできる。さらに、サービングIWFを無線ハブ内に併合することで、X-tunnelプロトコルを除去することもできる。

【０１２４】図２４は、登録フェーズ、つまり、エンドシステムの登録の際に用いられるプロトコルスタックをローカルAPセルアーキテクチャに対して示す。リモートAPセルアーキテクチャに対するプロトコルスタックもこれとほぼ同一である。上述のシナリオはローミングエンドシステムに対するものであり、ホームに位置するエンドシステムに対しては登録経路内にはフォーリン登録サーバは関与しない。

【０１２５】エンドシステム内のモビィリティエージェントについても説明の必要がある。エンドシステム内のモビィリティエージェントと無線ハブ内のフォーリンエージェントは、概念的に、mobile IP RFC 2002と類似する。このモビィリティエージェントは、ネットワークエラーをタイムアウトと再試行を用いて扱う。ベアラデータに対する周知のプロトコルスタックと異なり、RLP層は用いられない。フォーリンエージェントと登録サーバはエンドシステムの登録のためにRadius overUDP/IPを用いて互いに通信する。

【０１２６】セキュリティに関して幾つかの点を説明する必要がある。第一に、エンドシステムの識別とフォーリン／ホームネットワークの識別が、無線登録フェーズの際に認証（検証）される。第二に、エンドシステムの識別が自身のPPPサーバに対してPPP認証フェーズの際に認証（比較）される。第三に、アカウンティングデータの格納、課金、およびホームドメイン情報の更新の際に認証が行なわれる。第四に、エンドシステムとの間で送受されるベアラトラヒックは暗号化される。第五に、サービスプロバイダの境界を越えて課金情報を交換する際は暗号化が行なわれる。

【０１２７】無線登録の際のエンドシステムの識別のそれらのホームネットワークに対する認証（比較）およびホームネットワークとフォーリンネットワークの識別の認証には共有のセキュリティが用いられる。エンドシステムの認証においては、１２８ビットの共有のセキュリティを用いてその登録リクエストに対する認証子が生成される。この認証子は、mobile IPRFC 2002において指定される周知のMD５メッセージダイジェストアルゴリズムを用いて生成される。代替として、別のアルゴリズムを用いることもできる。エンドシステムは、この共有のセキュリティを登録リクエストに入れて送信することはなく、認証子のみを送信する。エンドシステムから登録リクエストを受信すると、ホーム登録サーバは、登録リクエストデータから共有のセキュリティを用いて認証子を再計算する。再計算した認証子の値がエンドシステムによって送信された認証子の値と一致する場合は、ホーム登録サーバは、以降の登録プロセスの進行を許可する。両方の値が一致しない場合は、ホーム登録サーバは、この事象を登録し、セキュリティ違反警告およびこのリクエストに対する否定通知（nak）を生成する。

【０１２８】登録応答を送り返すとき、ホーム登録サーバは上述と同一の手続きを遂行する。つまり、共有のセキュリティを用いて登録応答に対する認証子を生成し、これをエンドシステムに送信する。登録応答を受信すると、エンドシステムは共有のセキュリティを用いて認証子を再計算する。再計算した値がホーム登録サーバによって登録応答に入れて送られた認証子の値と一致しない場合は、エンドシステムは、その応答を破棄し、再び認証を試みる。

【０１２９】これらのネットワークセキュリティ概念は、mobile IP RFC 2002において定義されている概念と類似する。RFCによると、各エンドシステムとそのホームネットワークとの間には、モビィリティセキュリティアソシエーションが存在する。各モビィリティセキュリティアソシエーションは、セキュリティ文脈のコレクションを定義する。各セキュリティ文脈は、認証アルゴリズム、モード、セキュリティ（共有、公開、プライベート）、応答保護のスタイル、および用いる暗号化のタイプを定義する。本発明の背景においては、エンドシステムのUser-Nameが（ホームアドレスの代わりに）、各エンドシステムとそのホームネットワークとの間のモビィリティセキュリティアソシエーションを識別するために用いられる。セキュリティパラメータインデックス（SPI）と呼ばれるもう一つのパラメータがモビィリティセキュリティアソシエーション内の特定のセキュリティ文脈を選択するために用いられる。本発明の基本的な実施例においては、デフォルトmobile IP authenticationアルゴリズム（keyed-MD5）およびデフォルトモード（“prefix+suffix”）のみが１２８ビットの共有のセキュリティにてサポートされる。ネットワークユーザは、自身のホームネットワークとの間で複数の共有のセキュリティを定義することが許される。エンドユーザに対するセキュリティ文脈の生成、セキュリティパラメータインデックス（SPI）の各セキュリティ文脈への割り当て、セキュリティ文脈の内容（共有のセキュリティを含む）の設定、内容の修正等を遂行するための機構については後に説明する。登録の際に、エンドシステムは、１２８ービットのメッセージダイジェストを、接頭語＋接尾語モードにて、MD5アルゴリズムを用いて計算する。このとき、共有のセキュリティを登録リクエスト内の保護されるべきデータに対する接頭語および接尾語として用いる。次に、エンドシステムは、こうして計算した認証子を、SPIおよびUser-Nameと一緒に、登録リクエストに入れて送信する。エンドシステムの登録リクエストを受信すると、フォーリン登録サーバは、このリクエストを、認証子およびSPIと一緒に、変更を加えずに、ホーム登録サーバに中継する。エンドシステムから直接あるいはフォーリン登録サーバを介して間接的に登録リクエストを受信すると、ホーム登録サーバは、そのSPIおよびUser-Nameを用いてセキュリティ文脈を選択する。次に、ホームサーバは共有のセキュリティを用いて認証子を再計算する。再計算した認証子の値がエンドシステムによって登録リクエストに入れて送られた認証子の値と一致する場合は、ユーザの識別の認証は成功する。一致しない場合は、ホーム登録サーバは、エンドシステムによって送信された登録リクエストに対して否定の応答を送り返す。

【０１３０】ホーム登録サーバによってエンドシステムに送られる登録応答も上述のmobileIPアルゴリズムを用

いて認証（検証）される。ホームサーバは、SPIおよび計算した認証子の値を登録応答メッセージに入れてエンドシステムに送信する。登録応答を受信すると、エンドシステムは認証子を再計算し、再計算した値が送信した値と一致しない場合は、その登録応答を破棄し、再び認証を試みる。

【０１３１】ユーザのエンドシステムは、共有のセキュリティおよびユーザが自身の登録サーバと共有する全てのセキュリティ文脈に対するSPIを持つように構成する必要がある。このコンフィギュレーション情報は、好ましくは、Windows 95ベースのエンドシステムの場合は、Win 95レジストリに格納する。登録の際に、この情報がアクセスされ、認証の目的で用いられる。

【０１３２】ネットワーク内において、フォーリンエージェント（FA）は、エンドシステムに代わってエンドシステムの登録を行なうため、および無線ハブとホームIWFあるいはサービングIWFの間のxtunnelを構成するためにRadiusプロトコルを用いる。エンドシステムから登録リクエストを受信すると、FAは、Radius Access-Requestパケットを生成し、このパケット内に自身の属性を挿入し、さらに、エンドシステムの登録リクエストの属性を、変更を加えずに、このパケット内にコピーし、こうして結合したリクエストをMSC内の登録サーバに送信する。

【０１３３】Radius認証には、Radiusクライアント（この場合は基地局内のＦＡ）とRadiusサーバ（この場合はMSC内の登録サーバ）が、認証のためにセキュリティを共有することが必要とされる。この共有のセキュリティは、RadiusクライアントとRadiusサーバの間で通信されるプイラベート情報の暗号化にも用いられる。この共有のセキュリティは、コンフィガラブルなパラメータである。ネットワークは、Radius RFCの勧告に従って共有のセキュリティおよびMD5アルゴリズムを認証のために用い、暗号化が必要とされる場合は、暗号化のためにも用いる。FAによって送信されるRadius Access-Requestパケットは、Radius User-Name属性（これはエンドシステムによって供給される）およびRadius User-Password属性を含む。User-Password属性の値もコンフィガラブルな値であり、Radiusプロトコルによって勧告される方法に従って暗号化される。Radius RFC標準の観点からは非標準属性であるネットワークに特定な他の属性も、ベンダ固有のRadius属性として符号化され、Access-Requestパケットに入れて送信される。

【０１３４】FAは以下の属性をRadius Access-Requestパケットに挿入して登録サーバに送信する：

１．User-Name Attribute（ユーザ名属性）。これはエンドシステムのユーザ名であり、エンドシステムによって登録リクエストに入れて供給される。

２．User-Password Attribute（ユーザパスワード属性）。このユーザパスワードは、基地局／無線ハブによってユーザに代わって供給される。これは、Radius EFCの規定に従って基地局とその登録サーバとの間で共有されるセキュリティを用いて符号化される。

３．NAS-Port（NASポート）。これは基地局上のポートである。

【０１３５】４．NAS-IP Address（NAS-IPアドレス）。これは基地局のIPアドレスである。

５．Service-Type（サービスタイプ）。これはフレームドサービスである。

６．Framed Protocol（フレームドプロトコル）。これはPPPプロトコルである。

７．Xtunnel Protocol Parameters（Xtunnelプロトコルパラメータ）。これらのパラメータは基地局によってエンドシステムに代わってxtunnelプロトコルを設定するための必要なパラメータを指定するために送信される。これはベンダ固有の属性である。

８．AP-IP Address（AP-IP アドレス）。これはユーザが登録の際に用いるAPのIPアドレスである。これはベンダ固有の属性である。

【０１３６】９．AP-MAC-Address（AP-MACアドレス）。これはユーザが登録の際に用いるAPのMACアドレスである。

１０．End system's Registration Request（エンドシステムの登録リクエスト）。エンドシステムからの登録リクエストは、変更を加えず、このベンダ固有の属性内にコピーされる。

【０１３７】登録サーバは以下の属性をRadius Access-Responseパケットに入れてFAに送り返す：

１．Service Type（サービスタイプ）。これはフレームドサービスである。

２．Framed-Protocol（フレームドプロトコル）。これはPPPである。

３．Xtunnel Protocol Parameters（Xtunnelプロトコルパラメータ）。これらのパラメータは登録サーバによってエンドシステムに代わってxtunnelプロトコルを設定するために必要なパラメータを指定するために送られる。これはベンダ固有の属性である。

４．Home Resistration Server'Replay（ホーム登録サーバの応答）。この属性は、ホーム登録サーバからFAに送信される。FAは、この属性を、変更を加えずに、登録応答パケットに入れてエンドシステムに中継する。経路内にフォーリン登録サーバが存在する場合は、フォーリン登録サーバは、この属性を、変更を加えずに、FAに中継される。これはベンダ固有の属性として符号化される。

【０１３８】ローミングエンドシステムにサービスを提供するためには、フォーリンネットワークとホームネットワークが互いにアカウンティングおよび課金の目的で、認証とコンフィギュレーションのためにRadiusプロトコルを用いて認証（検証）される。この認証はエンド

システムが登録するときに遂行される。上述のように、フォーリンネットワーク内の登録サーバは、エンドシステムからの登録リクエスト（これはFAによってRadius-Access Requestパケット内にベンダ固有の属性としてカプセル化して中継される）を受信すると、このフォーリン登録サーバは、エンドシステムのNser-Nameを用いて、自身のホームドメインディレクトリ（HDD）を調べることで、エンドシステムのホーム登録サーバの識別を見つける。ホームドメインディレクトリ（HDD）には、以下の情報が格納されており、フォーリン登録サーバはエンドシステムの登録リクエストを転送するためにこれにアクセスする：

【０１３９】１．Home Registration Server IP Address（ホーム登録サーバのIPアドレス）。これは登録リクエストの転送先のホーム登録サーバのIPアドレスである。

２．Foreign Registration Server Machine Id（フォーリン登録サーバのマシンId）。これは、フォーリン登録サーバのSMTP（simplified mail transfer prorocol）フォーマットでのマシンIDである（これは、例えば、machine@fqdnの形式を持ち、マシン（machine）はフォーリン登録サーバマシンの名前を表し、fqdnはフォーリン登録サーバのドメインの完全修飾ドメイン名である）。

【０１４０】３．Tunneling Protocol Parameters（トンネリングプロトコルパラメータ）。これらは、エンドシステムに代わってサービングIWFとホームIWFとの間のトンネルを構成するためのパラメータである。これらパラメータには、これらの間で用いられるべきトンネリングプロトコルとトンネルを構成するためのパラメータが含まれる。

４．Shared Secret（共有のセキュリティ）。これはフォーリン登録サーバとホーム登録サーバとの間の認証のために用いられるべき共有のセキュリティである。このセキュリティは、フォーリン登録サーバからホーム登録サーバに送信されるRadius User-Password属性を計算するために用いられる。これは、２つの無線サーバプロバイダの間で定義される。

【０１４１】５．User-Password（ユーザパスワード）。これはローミングエンドシステムに代わって用いられるべきユーザパスワードである。このユーザパスワードは、２つの無線サービスプロバイダの間で定義される。このパスワードはRadius RFCの規定に従って共有のセキュリティを用いて暗号化される。

６．Accounting Parameters（アカウンティングパラメータ）。これらは登録するエンドシステムに代わって、アカウンティングを構成するためのパラメータである。これらパラメータは、登録サーバによって自身のIWFにエンドシステムに代わってアカウンティングを構成するために送信される。

【０１４２】フォーリン登録サーバは、上述の情報を用いてRadius Access-Requestを生成し、このRadius Access-Requestに自身の登録および認証情報を追加し、さらにこのRadius Access-Request内にエンドシステムから送信された登録情報を、変更を加えずに、コピーし、こうして結合したリクエストをホーム登録サーバに送信する。ホーム登録サーバは、Radius-Access Requestをエンドシステムがローミングしている場合はフォーリン登録サーバを介して受信し、エンドシステムがホームに位置する場合はFAから直接に受信するが、これを受信すると、後者の場合は自身のディレクトリサーバに照会して共有のセキュリティを得ることでエンドシステムの検証を行なう。一方、エンドシステムがローミングしている場合は、フォーリン登録サーバの識別を認証子を再計算することで検証する。

【０１４３】リクエストの認証に成功した場合は、ホーム登録サーバは、Radius Access-Accept応答パケットを生成し、これをエンドシステムがローミングしている場合はフォーリン登録サーバに送り返す。一方、エンドシステムがホームに位置する場合は、これをRadius-Access Requestを送信してきたFAに直接に送り返す。この応答には、登録応答属性が含まれ、FAは、これをエンドシステムに中継する。

【０１４４】他方、リクエストの認証に失敗した場合は、ホーム登録サーバは、Radius Access-Reject応答パケットを生成し、これを、エンドシステムがローミングしている場合はフォーリン登録サーバに返信する。一方、エンドシステムがホームに位置する場合は、Radius-Access Requestを送信してきたFAに直接に送り返す。この応答には、登録応答属性が含まれ、FAは、これをエンドシステムに中継する。

【０１４５】エンドシステムがローミングしているシナリオにおいては、ホーム登録サーバからの応答はフォーリン登録サーバによって受信され、これはフォーリン登録サーバによって共有のセキュリティを用いて認証（検証）される。認証の後に、フォーリン登録サーバは、応答を処理することで、自身のFAに送信するためのRadius応答パケット（AccessあるいはReject）を生成する。このとき、フォーリン登録サーバは、ホーム登録サーバによって返信されたRadius応答パケットからの登録応答属性を、変更を加えることなく、FAに送信するRadius応答パケット内にコピーする。

【０１４６】FAは、Radius Access-ResponseあるいはRadius Access-Reject応答パケットを受信すると、このRadius応答からの登録応答属性を用いて、登録応答パケットを生成し、この応答パケットをエンドシステムに送信する。これによってラウンドトリップ登録シーケンスが完了する。

【０１４７】Mobile IP標準は、登録応答の保護を、タイムスタンプを用いて、あるいはオプションしてノンス（nonces）を用いて実現することを指定する。ただし、

タイムスタンプを用いての応答の保護には、対応するノード間に正確に同期された日時クロックが要求される。このため、Mobile IP標準ではタイムスタンプの使用が強制でノンスの使用はオプションであるが、本発明では、登録の際の応答の保護はノンスを用いて実現される。ただし、代替として、タイムスタンプを用いて応答の保護を実現することも考えられる。

【０１４８】ノード間で用いられる応答保護のスタイルは、セキュリティ文脈内に認証文脈、モード、セキュリティ、暗号化のタイプと一緒に格納される。ネットワークはエンドシステムとそのPPPサーバとの間のPPPベースでのPAP（パスワード認証）およびCHAP（パスワード認証の挑戦）の使用をサポートする。これは、前述のmobile IPおよびRadiusベースの認証機構とは独立に行なわれる。これは、プライベートイントラネットあるいはISPがユーザの識別を独立に検証することを可能にする。

【０１４９】以下では、アカウンティングおよびディレクトリサービスに対する認証をアカウンティングセキュリティとの関連で説明する。同一MSC内のネットワーク装置からのディレクトリサーバへのアクセスの場合、認証は必要とされない。

【０１５０】ネットワークは、エンドシステムとホームIWFとの間で伝送されるベアラデータの暗号化をサポートする。エンドシステムは、該当するセキュリティ文脈を選択することで、暗号化がオンあるいはオフされることを指定する（協議する）。登録リクエストが受信されたとき、ホーム登録サーバは、エンドシステムの暗号化に対するリクエストをセキュリティ文脈に基づいて許可する。認証アルゴリズム、モード、共有のセキュリティ、および応答保護のスタイルを格納するのに加えて、セキュリティ文脈が用いるべき暗号化アルゴリズムのスタイルを指定するためにも用いられる。エンドシステムとホームエージェントとの間の暗号化が協議（指定）されている場合は、PPPフレーム全体を指定通りに暗号化した後に、これをRLPにカプセル化する。

【０１５１】IWF、アカウンティングサーバ、およびアカウンティングシステムは、MSC内の同一の信託されたドメイン（trusted domain）の一部分である。これらエンティティは、同一LAN上に接続されるか、あるいは無線サービスプロバイダによって所有および運用される信託されたイントラネットの一部分に接続される。IWFとアカウンティングサーバとの間、並びにアカウンティングサーバと顧客の課金システムとの間のアカウンティング統計の転送はIP-Sec.等のInternet IPセキュリティプロトコルを用いて暗号化する必要はない。

【０１５２】このネットワークでは、エンドシステムの位置をモニタすることは、より困難になる。これは、エンドシステムとの間で伝送される全てのPPPフレームが、エンドシステムデバイスの実際の位置と関係なく、ホームIWFを通過するように見えるためである。

【０１５３】アカウンティングデータは、ネットワーク内のサービングIWFとホームIWFによって集められる。サービングIWFによって集められたアカウンティングデータは、サービングIWFのMSC内のアカウンティングサーバに送られる。ホームIWFによって集められたアカウンティングデータは、ホームIWFのMSC内のアカウンティングサーバに送られる。サービングIWFによって集められたアカウンティングデータは、フォーリン無線サービスプロバイダによって、監査のため、および請求書を無線サービスプロバイダの境界間で清算するために用いられる（これによって、ローミングとモビィリティがサポートされる）。ホームIWFによって集められたアカウンティングデータは、エンドユーザに対する請求書を作成するために、および請求書を無線サービスプロバイダの境界間で、ローミングとモビィリティをサポートするために清算するために用いられる。

【０１５４】全てのデータトラヒックが、エンドシステムの位置およびフォーリンエージェントの位置に関係なく、ホームIWFに送られるために、ホームIWFは、顧客の請求書を生成するため、および、フォーリンネットワークの使用に関する清算情報を生成するための全ての情報を持つ。

【０１５５】サービングIWFおよびホームIWFは、登録したエンドシステムに対するアカウンティングレコードを送信するために、好ましくは、Radiusアカウンティングプロトコルを用いる。Radiusアカウンティングプロトコルは、ドラフトIETF RFCにおいて規定される通りである。本発明では、このプロトコルが拡張される。つまり、このRadius Accountingプロトコルに、このネットワークに対するベンダ固有の属性と、チェックポインティングが追加される。チェックポインティングとは、この背景においてはアカウンティングデータの定期的な更新を意味し、これによってアカウンティングレコードが失われる危険性を最小に押さえられる。

【０１５６】RadiusアカウンティングプロトコルはUDP/IP上でランし、確認応答（アクノレッジメント）とタイムアウトに基づく再試行を用いる。Radiusアカウンティングクライアント（サービングIWFあるいはホームIWF）は、UDPアカウンティングリクエストパケットを自身のアカウンティングサーバに送信する。すると、アカウンティングサーバは、アカウンティングクライアントに確認応答を送り返す。

【０１５７】ネットワーク内において、アカウンティングクライアント（サービングIWFおよびホームIWF）は、ユーザセッションが開始されるとアカウンティング開始指標を送信し、ユーザセッションが終了するとアカウンティング停止指標を送信する。アカウンティングクライアントは、さらに、セッション最中にもアカウンティングチェックポイント指標を送信する。これとは対照的に、IETF RFCドラフトRadiusアカウンティングは、アカ

ウンティングチェックポイント指標は指定しない。本発明のソフトウエアは、この目的のためにベンダ固有のアカウンティング属性を生成する。このアカウンティング属性は、Acct-Status-Type of Start（アカウンティング開始指標）を含む全てのRadius Accounting-Requestパケット内に存在する。この属性の値は、アカウンティングサーバに、そのアカウンティングレコードがチェックポインティングレコードであるか否かを通知するために用いられる。チェックポインティングアカウンティングレポートは、時間属性を持ち、セッションが開始されてからの累積アカウンティングデータを含む。本発明においては、チェックポインティングパケットの送信頻度はコンフィガラブルである。

【０１５８】サービングIWFおよびホームIWFは、各自の登録サーバによって、登録フェーズの際に、各自のアカウンティングサーバに接続されるように構成される。コンフィガラブルアカウンティングパラメータには、アカウンティングサーバのIPアドレスおよびUDPポート、チェックポインティングの頻度、セッション／マルチセッションのID、およびアカウンティングクライアントとアカウンティングサーバとの間で用いられるべき共有のセキュリティが含まれる。

【０１５９】ネットワークは、各登録したエンドシステムに対して、以下のアカウンティング属性を記録する。これらアカウンティング属性は、セッションの開始時、セッションの終了時、および中間（チェックポイント）において、アカウンティングクライアントによって、それらのアカウンティングサーバに、Radiusアカウンティングパケットに入れて報告される。このRadiusアカウンティングパケットは、以下を含む：

【０１６０】１．User Name（ユーザ名）。これは上述のRadius User-Name属性と類似する。この属性はユーザを識別するために用いられ、全てのアカウンティングレポート内に存在する。フォーマットは“user@domain”の形式を持ち、ドメインは（domain）は、ユーザのホームの完全修飾ドメイン名を表す。

２．NAS IP Address（NAS IP アドレス）。これは上述のNAS-IP-Address属性と類似する。この属性は、ホームIWFあるいはサービングIWFをランしているマシンのIPアドレスを識別するために用いられる。

【０１６１】３．Radio Port（無線ポート）。この属性はユーザにサービスを提供するアクセスポイント上の無線ポートを識別する。この属性はベンダ固有の属性として符号化される。

４．Access Point IP Address（アクセスポイントIPアドレス）。この属性はユーザにサービスを提供しているアクセスポイントのIPアドレスを識別する。この属性はベンダ固有の属性として符号化される。

５．Service Type（サービスタイプ）。これは上述のRadius Service-Type属性と類似する。この属性の値はFramedである。

【０１６２】６．Framed Protocol（フレームドプロトコル）。これは上述のRadius Framed-Protocol属性と類似する。この属性の値はPPPを示すように設定される。

７．Accounting Status Type（アカウンティング状態のタイプ）。これは上述のRadius Acct-Status-Type属性と類似する。この属性の値は、ユーザのRadiusクライアントとのセッションの開始を示すStart（開始）か、ユーザのRadiusクライアントとのセッションの停止を示すStop（停止）である。アカウンティングクライアントに対しては、Acct-Status-Type/Start属性はエンドシステムが登録したときに生成され、Acct-Status-type/Stop属性はエンドシステムがなんらかの理由で登録を解除したときに生成される。チェックポイントに対しては、この属性の値はStartであり、Accounting Checkpoint（アカウンティングチェックポイント）属性も存在する。

【０１６３】８．Accounting Session ID（アカウンティングセッションのID）。これは上述のRadius-Session-Idと類似する。エンドシステムがローミングしているシナリオでは、このセッションIDは、エンドシステムが登録リクエストを発行したときにフォーリン登録サーバによって割り当てられる。これは登録シーケンスの際にフォーリン登録サーバからホーム登録サーバに送信される。ホームネットワークとフォーリンネットワークの両方ともAcct-Session-ID属性を知っており、この属性を各自のアカウンティングサーバにアカウンティングレコードを送信する際に送信する。“エンドシステムがホームに存在する”シナリオでは、この属性はホーム登録サーバによって生成される。ホーム登録サーバは、この属性の値を、自身のIWFに通知する。すると、IWFはこれを全てのアカウンティングレコード内に挿入する。

【０１６４】９．Accounting Multi-Session ID（アカウンティングマルチセッションのID）。これは上述のRadius Acct-Multi-Session-IDと類似する。このIDは、ホーム登録サーバによって、エンドシステムに代わって登録リクエストがFAから直接に受信されたとき、あるいはこれがフォーリン登録サーバを介して受信されたときに割り当てられる。これはホーム登録サーバからフォーリン登録サーバに登録応答メッセージに挿入して送られる。フォーリン登録サーバは、この属性の値を、自身のIWFに送り、IWFはこれを全てのアカウンティングレコードに挿入する。

【０１６５】アーキテクチャに真のモビィリティが追加されるが、このIDは、エンドシステムが、あるIWFから別のIWFに移動した場合に、同一のエンドシステムに対する異なるIWFからのアカウンティングレコードを一つに纏めるために用いられる。IWF境界間でハンドオフした場合、IWFが変わると アカウンティングレコード内のAcct-Session-Idも変わる。ただし、Acct-Multi-Session-Idの属性は、そのユーザにサービスを提供した全ての

IWFが、アカウンティングレコード内に同一の値を用いる。セッションIDとマルチセッションIDは、フォーリンネットワークとホームネットワークの両方によって知られていおり、両ネットワークはこれらの属性をアカウンティングレポートに挿入し、各自のアカウンティングサーバに送る。課金システムはこれらセッションIDおよびマルチセッションIDを用いて同一無線サービスプロバイダのIWF境界間あるいは異なる無線サービスプロバイダの境界間からのアカウンティングレコードを一つに纏める。アカウンティングレコードには以下が含まれる：

【０１６６】１．Accounting Delay Time（アカウンティング遅延時間）。Radius Acct-Delay-Timeの属性を参照されたい。

２．Accounting Input Octets（アカウンティング入力オクテット）。RadiusAcct-Input-Octetsを参照されたい。この属性はエンドシステムから送信される（エンドシステムからネットワークに入力される）オクテットの数を追跡するために用いられる。このカウントは、もっぱらPPPフレームを追跡するために用いられ、エアリンクのオーバーヘッドや、RLPその他によって生じるオーバヘッドはカンウトされない。

【０１６７】３．Accounting Output Octets（アカウンティング出力オクテット）。RadiusAcct-Output Octetsを参照されたい。この属性はエンドシステムに送られる（ネットワークからエンドシステムに出力される）オクテットの数を追跡するために用いられる。このカウントはもっぱらPPPフレームを追跡するために用いられ、エアリンクのオーバーヘッドや、RLPその他によって生じるオーバヘッドはカンウトされない。

【０１６８】４．Accounting Authentic（アカウンティング認証）。Radius Acct-Authenticの属性を参照されたい。この属性の値はそのアカウンティングレコードがサービングIWFによって生成されたかホームIWFによって生成されたかにによってLocal（ホーム）かRemote（フォーリン）のいずれかを取る。

５．Accounting Session Time（アカウンティングセッション時間）。RadiusAcct-Session Timeの属性を参照されたい。この属性はユーザがサービスを受けた時間の量を示す。サービングIWFによって送信された場合は、この属性はユーザがそのサービングIWFからサービスを受けた時間の量を追跡する。ホームIWFによって送信された場合は、この属性はユーザがそのホームIWFからサービスを受けた時間の量を追跡する。

【０１６９】６．Accounting Input Packets（アカウンティング入力パケット）。Radius Acct-Input Packetsの属性を参照されたい。この属性はエンドシステムから受信されたパケットの数を追跡する。サービングIWFの場合は、この属性はエンドシステムからそのサービングIWFに入力されたPPPフレームの数を追跡する。ホームIWFの場合は、この属性はエンドシステムからそのホームIWFに入力されたPPPフレームの数を追跡する。

【０１７０】７．Accounting Output Packets（アカウンティング出力パケット）。RadiusAcct-Output Packetsの属性を参照されたい。この属性はエンドシステムに送信されたパケットの数を示す。サービングIWFの場合は、そのサービングIWFからエンドシステムに送信されたPPPフレームの数を追跡する。ホームIWFの場合は、この属性はそのホームIWFからエンドシステムに送信されたPPPフレームの数を追跡する。

【０１７１】８．Accounting Terminate Cause（アカウンティング終端原因）。Radius Acct-Causeの属性を参照されたい。この属性はユーザセッションが終端された理由を示す。加えて、追加の詳細を与えるために特定の原因コードも存在する。この属性はセッション終端時のアカウンティングレポート内にのみ存在する。

【０１７２】９．Network Accounting Terminate Cause（ネットワークアカウンティング終端原因）。この属性はセッションが終端された詳細な理由を示す。この特定属性はベンダ固有の属性として符号化され、セッション終端時のみにRadius Accounting属性内に挿入して報告される。標準Radius属性であるAcct-Terminate Causeも存在する。この属性はAcct-Terminate Cause属性によってはカバーされない特定な原因コードを提供する。

【０１７３】１０．Network Air link Access Protocol（ネットワーク空中リクンアクセスプロトコル）。この属性はエンドシステムによって用いられるエアリンクアクセスプロトコルを示す。この属性はベンダ固有の属性として符号化される。

１１．Network Backhaul Access Protocol（ネットワークバックホールアクセスプロトコル）。この属性はアクセスポイントとエンドシステムとの間でデータを送受するために用いられるバックホールアクセスプロトコルを示す。この属性はベンダ固有の属性として符号化される。

【０１７４】１２．Network Agent Machine Name（ネットワークエージェントマシン名）。これはホームIWFあるいはサービングIWFをランするマシンの完全修飾ドメイン名である。この特定属性はベンダ固有の属性として符号化される。１３．Network Accounting Check-point（ネットワークアカウンティングチェックポイント）。RFCドラフトRadiusアカウンティングは、チェックポイントパケットは定義しないために、本発明によるネットワークは、Radiusアカウンティング開始パケット内にこの属性を用いることでチェックポイントをマークする。このチェックポイント属性の存在しない場合は、従来のアカウンティング開始パケットであることを意味する。アカウンティング開始パケット内にこの属性が存在する場合は、それがアカウンティングチェックポイントパケットであることを意味する。アカウンティング停止パケットの場合はこの属性は含まない。

【０１７５】好ましい実施例においては、全てのアカウンティングパケットおよび対応する確認応答は、MD5および共有のセキュリティを用いて認証（検証）されることを必要とする。IWFは共有のセキュリティを備えるように構成され、IWFは自身のRaiusアカウンティングサーバと通信する際に、この共有のセキュリティを認証のために用いる。IWFによってアカウンティングサーバと通信するために用いられる共有のセキュリティは、MSC内に位置するホーム／フォーリンドメインディレクトリ内に格納される。アカウンティングセキュリティのために用いられるこれら共有のセキュリティは、エンドシステムの登録シーケンスの際に、登録サーバからIWFに送られる。

【０１７６】アカウンティングサーバソフトウエアはMSC内に位置するコンピュータ内でランする。システム内でのアカウンティングサーバの役割は、ネットワーク要素（ホームIWFおよびサービングIWF）から生のアカウンティングデータを集め、このデータを処理および格納し、その後、これを無線サービスプロバイダの課金システムに転送することにある。アカウンティングサーバは、課金システムは含まず、これは、自動あるいは手動のアカウンティングデータ転送機構をサポートする。自動のアカウンティングデータ転送機能を用いる場合は、アカウンティングサーバは、アカウンティングレコードを、AMA課金フォーマットにて、顧客の課金システムにTCP/IPトランスポート層を通じて転送する。この目的のために、システムはパケットデータに対するAMA課金レコードフォーマットを定義する。手動の転送機構を用いる場合は、顧客は、アカウンティングレコードを課金システムに転送するためのテープを構築する。顧客の仕様に合わせてテープが構築できるように、顧客にはアカウンティングレコードにアクセスするための情報が提供される。顧客はこの情報を用いてアカウンティングレコードを処理し、これをテープに書き込む。

【０１７７】図２５は、ホームIWFあるいはサービングIWFからアカウンティングサーバによって受信された生のアカウンティングデータが、アカウンティングサーバによって処理および格納される様子を示す。アカウンティングサーバによって遂行される処理には、IWFから受信された生のアカウンティングデータのフィルタリング、圧縮、および相関が含まれる。現用／待機二重のプロセッサと、ホットスワップが可能な高速ディスクとを用いる高アビイラビィリティのファイルサーバが、アカウンティングデータをアカウンティングサーバに送信する際に、データを一時的に緩衝するために用いられる。

【０１７８】アカウンティングサーバは、生のアカウンティングデータの処理を、エンドシステムがそのmobile IPセッションを終了するまで遅延させる。エンドシステムがセッションを終了すると、アカウンティングサーバはそのセッションを通じて集められた生のアカウンティングデータを処理し、アカウンティングサマリ（要約）レコードを、SQLデータベースに格納する。SQLデータベースに格納されるアカウンティングサマリレコードは、ASN.1符号化されたファイル（ASN.1 encodedfile）をポイントする。このファイルは、エンドシステムのセッションに関する詳細なアカウンティング情報を含む。アカウンティングサーバ内に格納されたデータは、次に、課金データ転送エージェントによって顧客の課金システムに転送される。別の方法として、無線サービスプロバイダがアカウンティングデータをSQLデータベースおよび／あるいはASN.1符号化されたファイルからテープを介して課金システムに転送することもできる。データベーススキームとASN.1符号化されたファイルのフォーマットが、顧客がこれを利用できるようにドキュメント化され、顧客に供給される。アカウンティングシステム内に格納されている処理済みのアカウンティングデータの量が高水位マークを超えると、アカウンティングサーバはNMS警告を発行する。この警告はアカウンティングサーバ内に格納されているデータの量が低水位マーク以下に落ちると解除される。警告を発する高水位マークおよび警告を解除する低水位マークは、コンフィガラブルである。アカウンティングサーバは格納されているアカウンティングデータの年令があるコンフィガラブルな閾値を超えた場合も、NMS警告を発行する。逆に、この警告はアカウンティングデータの年令がこの閾値以下に落ちたときは解除される。

【０１７９】加入者ディレクトリは、加入者に関する情報を格納するために用いられ、ホームネットワーク内に設置される。ホーム登録サーバは、登録フェーズの際に、エンドシステムの認証および登録のために、このディレクトリを調べる。各加入者に対して、加入者ディレクトリは、以下の情報を格納する：

【０１８０】１．User-Name（ユーザ名）。加入者レコード内のこの欄は、SMTPフォーマット（例えば、user@fqdn）の形式を持ち、userサブ欄は、加入者を加入者の無線ホームドメインにて識別し、fqdnサブ欄は、加入者の無線ホームドメインを識別する。この欄は、エンドシステムによって登録フェーズの際に登録リクエストに挿入して送信される。この欄は、無線サービスプロバイダによって加入者にネットワークサービスに加入するときに割り当てられる。この欄はPPPにおいて用いられるユーザ名欄とは異なる。

【０１８１】２．Mobility Security Association（モビィリティセキュリティアソシエーション）。加入者レコード内のこの欄は、加入者とそのホームネットワークとの間のモビィリティセキュリティアソシエーションを含む。上述のように、各加入者とそのホーム登録サーバとの間には、モビィリティセキュリティアソシエーションが存在する。このモビィリティセキュリティアソシエーションは、セキュリティ文脈のコレクションを定義

し、各セキュリティ文脈は、認証アルゴリズム、認証モード、共有のセキュリティ、応答保護のスタイル、およびエンドシステムとホームサーバとの間で用いるべき暗号化のタイプ（無暗号化も含む）を含む。登録の際、ホーム登録サーバは、エンドシステムによって登録リクエストに挿入して供給されるUser-Nameおよびsecurity parameter index（SPI）を用いてこの加入者ディレクトリからその加入者のセキュリティ文脈に関する情報を取り出す。このセキュリティ文脈内の情報は、そのセッションの際の認証（検証）、暗号化および応答の保護を強化するために用いられる。このモビィリティセキュリティアソシエーションは、無線サービスプロバイダによって加入の際に生成される。加入者がこのアソシエーションを修正することを許可するか否かは、無線サービスプロバイダに一任される。許される場合は、加入者は、顧客サービス係りに電話したり、secure Web site（セキュリティウエブサイト）にアクセスすることで、モビィリティセキュリティアソシエーションの内容を確認あるいは修正する。加えて、加入者は、サービスプロバイダによって許される他の加入者情報にアクセスすることもできる。

【０１８２】３．Modem MAC Address（モデムMACアドレス）。この欄は加入者によって所有されるモデムのMACアドレスを含む。登録の際に、共有のセキュリティに加えてこの欄もユーザを認証（検証）するために用いられる。このMACアドレスに基づく認証は、ユーザベースでオフすることもできる。このMACアドレスは登録の際にホーム登録サーバに送信される。

【０１８３】４．Enable MAC address Authentication（MACアドレス認証起動）。この欄は、MACアドレスに基づく認証が、enabled（起動）されているか、disabled（不能）にされているかを決定するために用いられる。enabled（起動）されている場合は、ホーム登録サーバは、登録を試みているエンドシステムのMACアドレスをこの欄に対してチェックすることで、エンドシステムの識別を検証する。disabled（不能）にされている場合は、このチェックは行なわれない。

【０１８４】５．Roaming Enabled Flag（ローミング起動標識）。この欄がenabled（起動）に設定されている場合は、エンドシステムは、フォーリンネットワークにローミングすることを許される。この欄がdisabled（不能）にされている場合は、エンドシステムは、フォーリンネットワークにローミングすることは許されない。

６．Roaming Domain List（ローミングドメインリスト）。この欄はRoaming Enabled Flagがenabled（起動）に設定されている場合にのみ意味を持つ。この欄は、エンドシステムがそこにローミングすることを許されるフォーリンドメインのリストを含む。このリストの内容がナル（空）で、しかも、Roaming Enabled Flagがenabled（起動）に設定されている場合は、そのエンドシステムは、自由にローミングすることを許される。

【０１８５】７．Service Enable/Disable Flag（サービス起動／不能標識）。この欄は、システム管理者によって、加入者へのサービスを不能にするためにdisabled（不能）に設定することができる。この欄がenabled（起動）に設定されている場合は、加入者はサービスを受けるために登録することを許される。加入者が登録した後に、この欄の値がdisabled（不能）に設定された場合は、その加入者のエンドシステムは、ネットワークによって即座に切断される。

【０１８６】８．Internet Service Provider Association（インターネットサービスプロバイダアソシエーション）。この欄は加入者のインターネットサービスプロバイダに関する情報を含む。この情報はIWFによって、PPP登録フェーズの際に、エンドシステムに代わってインターネットサービスプロバイダを認証（検証）し、インターネットサービスプロバイダのPPPサーバとの間にL2TPトンネルを生成するために用いられる。この欄は加入者のISPの識別を含む。IWFは、この識別情報を用いて、エンドシステムに代わって認証とL2TPトンネルの設定を遂行するためにISPのディレクトリにアクセスする。

【０１８７】９．Subscriber's Name &; Address Information（加入者の名前およびアドレス情報）。この欄は加入者の名前、アドレス、電話、ファックス、ｅーメールアドレス等を含む。ホームドメインディレクトリ（HDD）は、登録サーバによって、エンドシステムに代わって登録を完結するためにエンドシステムに関するパラメータを調べるために用いられる。登録サーバは、この情報を用いて、エンドシステムがホームから登録しているのか、あるいはそのエンドシステムがローミングエンドシステムであるかを決定する。ホームのエンドシステムである場合は、登録サーバはホーム登録サーバの役割を担い、エンドシステムの登録を行なう。ローミングエンドシステムである場合は、登録サーバはフォーリン登録サーバの役割を担い、Radius代理（プロキシ）として機能し、実際のホーム登録サーバの識別をこのディレクトリから調べ、そのホーム登録サーバに登録リクエストを転送する。このHDD内に格納されてい るローミングエンドシステムの場合に用いられるパラメータとしては、ホーム登録サーバのIPアドレス、ホームとフォーリンによって共有されるセキュリティ、ホームIWFとサービングIWFとの間のトンネルコンフィギュレーション等が含まれる。このHDDはMSC内に位置する。

【０１８８】このHDD内には以下の情報が格納されている：

１．Home Domain Name（ホームドメイン名）。この欄はエンドシステムによって登録リクエストに入れて供給された完全修飾ホームドメイン名と一致するHDD内のエントリを探すためのキーとして用いられる。

２．Proxy Registration Request（代理登録リクエス

ト）。この欄は登録サーバによってそれがフォーリン登録サーバとして機能すべきか否かを決定するために用いられる。真である場合は、フォーリン登録サーバとして機能し、エンドシステムの登録リクエストを実際のホーム登録サーバに中継する。

【０１８９】３．Home Registration Server DNS Name（ホーム登録サーバのDNS名）。proxy registration request標識がTRUE（真）である場合は、フォーリン登録サーバは、この欄を用いて実際のホーム登録サーバのDNS名にアクセスする。真でない場合は、この欄は無視される。このDNS名はフォーリン登録サーバによってIPアドレスに翻訳される。フォーリン登録サーバはこのIPアドレスを用いて、エンドシステムの登録リクエストを中継する。

【０１９０】４．Foreign Domain Name（フォーリンドメイン名）。proxy registration request 標識がTRUE（真）である場合は、フォーリン登録サーバは、この欄を用いてフォーリンドメイン名に対応するエンドシステムのホーム登録サーバを識別する。真でない場合は、この欄は無視される。フォーリン登録サーバは、こうして得られた情報を用いて、フォーリンサーバマシンidをSMTPフォーマット、例えば、machine@fqdnの形式にて生成する。フォーリン登録サーバから、このマシンidをRadius-Access Reuestに挿入してホーム登録サーバに送信する。

【０１９１】５．Shared Secret（共有のセキュリティ）。proxy registration request 標識がTRUE（真）である場合は、この共有のセキュリティを用いて、フォーリン登録サーバとホーム登録サーバとの間で互いの識別が認証（検証）される。真でない場合はこの欄は無視される。

６．Tunneling Protocol Parameters（トンネリングプロトコルパラメータ）。この欄はエンドシステムにサービスを提供するためのトンネルを構成するために用いられる。ホームのエンドシステムに用いるパラメータとしては、基地局とホームIWFとの間、並びにホームIWFからPPPサーバへのトンネルに関する情報が含まれる。ローミングエンドシステムに用いるパラメータとしては、基地局からサービングIWFへの並びにサービングIWFからホームIWFへのトンネリングに関する情報が含まれる。この欄は各トンネルに対して、最小でも、用いるべきトンネリングプロトコルのタイプおよび任意のトンネリングプロトコルに特定なパラメータを含む。例えば、この欄はトンネリングプロトコルL2TPに対する識別子およびIWFとその相手（ピア）との間でL2TPトンネルを構成するために必要な追加のパラメータを含む。

【０１９２】７．Accounting Server Association（アカウンティングサーバアソシエーション）。この欄はIWFによってエンドシステムに代わってアカウンティングデータを生成するために必要な情報を格納するために用いられる。これには、アカウンティングプロトコルの名前（例えば、RADIUS）、アカウンティングサーバのDNS名およびそのアカウンティングプロトコルに固有のUDPポート番号等の追加のパラメータ、IWFがRadius Accountingプロトコル内に用いることを要求される共有のセキュリティ、チェックポインティングの頻度、セッション／マルチセッションidを生成するためのシード（種）等が含まれる。このアカウンティングサーバのDNS名は、アカウンティングサーバのIPアドレスに翻訳され、IWFに送信される。

【０１９３】互いにローミング合意を持つ無線サービスプロバイダの場合は、このHDDは、登録プロセスの認証（検証）および完結に用いられる。エンドシステムが自身のホームネットワークからフォーリンネットワークにローミングした場合は、フォーリンネットワーク内のフォーリン登録サーバは、訪問してきたエンドシステムにサービスを提供する前に、自身のMSC内のHDDを調べ、訪問（ローミング）しているエンドシステムのホーム登録に関する情報を得てホームネットワークの認証（検証）を行なう。

【０１９４】ホームドメインディレクトリ管理に対するソフトウエアは、好ましくは、システム管理者に対して、グラフィカルユーザインタフェース（graphical user interface、GUI）に基づくHDD管理を提供する。システム管理者はこのGUIを用いてHDD内のエントリの確認や更新を行なう。ただし、このGUIはフォーリン無線ネットワークサービスプロバイダがローミング合意に基づいてリモートから更新を行なうためには意図されていない。これは、もっぱら、防火壁の内側で作業するホーム無線サービスプロバイダの信託された（トラステッド）従業員によって用いられることのみを意図される。

【０１９５】フォーリンドメインディレクトリ（FDD）は、ホームドメインディレクトリとは反対の機能を提供する。FDDはホーム登録サーバによって用いられる。つまり、ホーム登録サーバは、FDDからフォーリン登録サーバおよびフォーリンネットワークに関するパラメータを取り出し、フォーリンネットワークの認証（検証）やサービングIWFとホームIWFとの間のトンネルの生成の際にこれを用いる。これらパラメータには、ホームネットワークとフォーリンネットワークの間の共有のセキュリティや、ホームIWFとサービングIWFとの間のトンネルコンフィギュレーション等が含まれる。このFDDはホーム登録サーバのMSC内に位置する。このFDDはホーム登録サーバによってローミングエンドシステムの登録に用いられる。

【０１９６】このFDDには以下の情報が格納される：

１．Home Domain Name（ホームドメイン名）。この欄はエンドシステムを中継しているフォーリン登録サーバの完全修飾ドメイン名と一致するFDD内のエントリを探すためのキーとして用いられる。

２．Shared Secret（共有のセキュリティ）。これはフォーリン登録サーバとホーム登録サーバとの間で互いの識別を互いに認証（検証）するために用いられる共有のセキュリティである。

【０１９７】３．Home IFW-Serving IWF Tunneling Protocol Parameters（ホームIWFとサービングIWFの間のトンネリングプロトコルパラメータ）。この欄はホームIWFとサービングIWFとの間でトンネルを構成するために用いられる。この欄は、最小でも、用いるべきトンネリングプロトコルのタイプおよび任意のトンネリングプロトコルに特定なパラメータを含む。例えば、この欄はトンネリングプロトコルL2TPに対する識別子およびサービングIWFとホームIWFとの間でL2TPトンネルを構成するために必要な追加のパラメータを含む。

【０１９８】４．Accounting Server Association（アカウンティングサーバアソシエーション）。この欄はホームIWFによってエンドシステムに代わってアカウンティングデータを生成するために必要な情報を格納するために用いられる。これには、アカウンティングプロトコルの名前（例えば、RADIUS）、アカウンティングサーバのDNS名およびそのアカウンティングプロトコルに固有のUDPポート番号等の追加のパラメータ、IWFがRadius Accountingプロトコル内に用いることを要求される共有のセキュリティ、チェックポインティングの頻度、セッション／マルチセッションidを生成するためのシード（種）等が含まれる。このアカウンティングサーバのDNS名は、アカウンティングサーバのIPアドレスに翻訳され、IWFに送信される。

【０１９９】互いにローミング合意を持つ無線サービスプロバイダの場合は、このFDDは、登録プロセスの認証（検証）および完結に用いられる。エンドシステムが自身のホームネットワークからフォーリンネットワークにローミングした場合は、ホームネットワーク内の登録サーバは、自身のMSC内のFDDを調べ、エンドシステムにサービスを提供しているフォーリンネットワークに関する情報を得てフォーリンの認証（検証）を行なう。

【０２００】このフォーリンドメインディレクトリ管理ソフトウエアは、好ましくは、システム管理者に対して、グラフィカルユーザインタフェース（GUI）に基づくFDD管理を提供する。システム管理者はこのGUIを用いてHDD内のエントリの確認や更新を行なう。ただし、このGUIはフォーリン無線ネットワークサービスプロバイダがローミング合意に基づいてリモートから更新を行なうためには意図されていない。これは、もっぱら、防火壁の内側で作業するホーム無線サービスプロバイダの信託された（トラステッド）従業員によって用いられることのみを意図される。

【０２０１】ホームIWFはインターネットサービスプロバイダディレクトリ（ISPD）を用いて、無線サービスプロバイダとサービス合意を持つISPとの間の接続性を管理し、加入者がそのネットワークを用いて自身のISPにアクセスできるようにする。各加入者に対して、加入者ディレクトリはその加入者のISPに対するエントリを持ち、この欄は、ISPD内のエントリをポイントする。ホームIWFはこの情報を用いて加入者に代わってISPへの接続を設定する。

【０２０２】このネットワークアーキテクチャはローミングをサポートする。複数の無線サービスプロバイダの間でローミングが機能するためには、このアーキテクチャは、無線サービスプロバイダ間のローミング合意の設定をサポートできる必要がある。このためには、２つの要件、つまり：（１）複数の無線サービスプロバイダを横断してシステムディレクトリを更新できること、および（２）無線サービスプロバイダ間で請求書（料金）を清算できることが必要となる。

【０２０３】加入者がインターネットサービスプロバイダにアクセスできるようにするために、このネットワークアーキテクチャは、インターネットサービスプロバイダとの間にローミング合意を持つ。このためには、このネットワークアーキテクチャは、ISPのPPPサーバとの間でデータが授受できる必要がある（つまり、PPP、L2TP、Radius等の標準プロトコルをサポートできる必要がある）。このアーキテクチャはさらにISPアクセスに対するディレクトリの更新や、ISPとの間での料金の清算を扱える必要がある。

【０２０４】２つの無線サービスプロバイダの間でローミング合意が確立されると、両方のプロバイダは、他のネットワークからそのネットワークに訪問するエンドシステムに対する認証および登録機能をサポートするために、ホームおよびフォーリンドメインディレクトリを更新することが必要となる。本発明のネットワークアーキテクチャは、最小の場合は、手動のディレクトリ更新をサポートする。この方法においては、２つの無線サービスプロバイダの間でローミング合意が確立されると、合意した２つのパーティは、それらのホームおよびフォーリンドメインディレクトリに入力するための情報の交換を行なう。この方法では、これらディレクトリの実際の更新は、各サービスプロバイダの従業員によって手動で行なわれる。後になってホームおよびフォーリンドメインディレクトリ内の情報を更新することが必要になった場合は、合意した２つのパーティは、更新情報を交換し、これらの更新を手動でディレクトリに入力する。

【０２０５】代替の実施例においては、ディレクトリ管理ソフトウエアは、インターネットサービスプロバイダ間のローミングを可能にするとともに、ISPがローミング関係を自動的に管理および発見することを可能にするIETF標準の開発（developingstandards in IETF）を組み込む。この場合は、手動でのディレクトリ管理は不要となる。ネットワークシステムがローミング関係の伝搬、ローミング関係の発見、訪問するエンドシステムの

認証および登録を自動的に遂行する。

【０２０６】アカウンティングデータの処理については、ネットワークアーキテクチャは、最小の場合は、単にアカウンティング情報の処理、格納、および無線サービスプロバイダの課金システムへのデータの送信のみをサポートし、ローミングに対する料金の清算は、課金システムに任される。代替の実施例においては、インターネットサービスプロバイダの間にアカウンティングレコードを配送するIETF標準を開発（developing standards in IETF）がネットワークアーキテクチャ内に組み込まれ、ISPがローミングエンドシステムに対する料金の清算を行なうことが可能にされる。

【０２０７】システムソフトウエアは、ISPおよびプライベートイントラネットへのアクセスのサポートを、ホームIWFとISPのあるいはイントラネットのPPPサーバの間にL2TPをサポートすることで実現する。インターネットサービスプロバイダディレクトリ（ISPD）は、IWFがこれらトンネルを生成するために必要とされる情報を含む。無線サービスプロバイダとインターネットサービスプロバイダとの間でアクセス合意が行なわれると、このディレクトリは無線サービスプロバイダの従業員によって手動で更新される。無線サービスプロバイダとインターネットサービスプロバイダとの間のアクセス関係の自動的な更新および発見も現在開発されており、インターネット標準の進化に合わせて実現される見込みである。現時点ではインターネットサービスプロバイダにアクセスすると、加入者は２つの請求書を受け取る。つまり、第一は無線サービスプロバイダから無線ネットワークの使用に対して受け取り、第二はインターネットサービスプロバイダから受け取る。両方のタイプの料金を結合する（一つに纏める）共通の請求書は、この最小実現のソフトウエアでは扱われないが、将来的にはこのソフトウエアに料金清算のためのインターネット標準をこれらの進化に合わせて組み込み、加入者がISPと無線サービスプロバイダとの間のローミング合意に基づいて共通の請求書を受け取るようにすることも見込まれる。

【０２０８】本発明のシステムはネットワーク要素を管理するための要素管理システムを含む。システム管理者は、要素マネージャから構成、性能および故障／警告管理機能を遂行する。要素管理アプリケーションは、ウエブブラウザ上でランする。ウエブブラウザを用いて、システム管理者はTCP/IPアクセスが可能な任意の場所からネットワークを管理する。要素マネージャは上位レベルのマネージャに対するエージェントの役割も遂行する。この役割の中で要素マネージャは警告および故障監視のためにSNMP MIB（Simple Network Manegement Protocol／Management Information Base）をエクスポートする。

【０２０９】上位レベルのSNMPマネージャは、SNMPトラップを介して警告状態を通知される。上位レベルのSNMPマネージャは定期的に要素マネージャのMIBにネットワークの健康（健全性）および状態について問い合せる。この上位レベルのSNMPマネージャの所のシステム管理者は、ネットワークのアイコンレプレゼンテーショ（アイコンによるネットワーク表現）とその現在の警告状態を監視することができる。特定のネットワーク要素アイコンをポイントし、クリックすることで、システム管理者は、ウエブブラウザを用いて要素管理アプリケーションを実行し、より細部の管理機能を遂行する。

【０２１０】ネットワーク内においては、物理的および論理的ネットワーク要素の管理は、SNMPプロトコルと内部管理用アプリケーションプログラミングインタフェースを用いて遂行される。要素マネージャ内のアプリケーションはSNMPあるいは他の管理API（Application Programming Interface）を用いてネットワーク管理機能を遂行する。アーキテクチャ上は、要素管理システムには２つの異なるセットの機能要素が含まれる。第一のセットの機能要素には、コンフィギュレーションデータサーバ、パフォーマンスデータモニタ、健康／状態モニタ、およびネットワーク要素回復ソフトウエアが含まれ、これらはRAIDディスクを備えるHAサーバ上でランする。第二のセットの機能要素には、専用の非ーHA管理システム上で実行する管理アプリケーションが含まれる。要素マネージャシステムが動作不能となった場合でも、これらネットワーク要素は引き続いてランし、警告を報告したり、さらには、故障状態を回復することができる。ただし、全ての管理アプリケーションは非ーHAの要素マネージャ内で実行し、要素マネージャが故障した場合、人の介在を要求する回復動作は、要素マネージャが動作可能となるまでは不可能になる。

【０２１１】基地局内の無線ハブ（WH）は典型的には無線サービスプロバイダ（WSP）によって所有され、これらはWSPの登録サーバ（RS）にポイント・ツウ・リンク、イントラネット、あるいはインターネットによって接続される。WSPの登録サーバは、典型的には、プロセッサ上で実行し、幾つかの登録機能を遂行するソフトウエアモジュールである。インターワーキング機能ユニット（IWFユニット）は、典型的には、プロセッサ上で実行し、幾つかのインタフェーシング機能を遂行するソフトウエアモジュールである。IWFユニットは、典型的には登録サーバにイントラネット／WANを介して接続され、IWFユニットは典型的にはWSPによって所有される。ただし、IWFユニットは、必ずしも登録サーバと同一のLAN内に位置する必要はない。典型的には、アカウンティングサーバおよびディレクトリサーバは（プロセッサ上で実行するソフトウエアモジュールも含めて）登録サーバに、サービスプロバイダのデータセンタ（例えば、様々なサーバおよび他のソフトウエアをホストする一つあるいは複数のプロセッサを含むセンタ）内のLANを介して接続される。エンドシステムからのトラヒックは（こ

のLANに接続された）ルータを介して公衆インターネットるいはISPのイントラネットにルートされる。フォーリンWSPのネットワーク内に位置する登録サーバはフォーリン登録サーバ（FRS）と呼び、エンドシステムのホームネットワーク（そのモバイルがそのサービスを購入する所のネットワーク）内に位置する登録サーバはホーム登録サーバ（HRS）と呼ぶ。また、ホームネットワーク内のインターネットワーキング機能ユニットはホームIWFと呼び、フォーリンネットワーク（つまりエンドシステムの訪問先のネットワーク）内のインターワーキング機能ユニットはサービングIWFと呼ぶ。

【０２１２】固定無線サービス（つまり、移動しないエンドシステム）の場合は、エンドシステムはホームネットワークのサービスを求めて、ホームネットワークから（例えば、アットホームサービス：at home service）、あるいはフォーリンネットワークから（例えば、ローミングサービス：roaming service）登録する。エンドシステムは無線ハブ内のエージェント（例えば、ソフトウエアにて実現されたエージェント機能）から送信されるアドバタイズメントをアクセスポイントを介して受信する。この際に、MAC層の登録とネットワーク層の登録の両方を遂行することが必要となる。これらは、効率を良くするために互いに結合することもできる。

【０２１３】ホームに位置するエンドシステムの場合（図２６）は、ネットワーク層の登録は（ローカルな登録のように）、ホーム登録サーバに、エンドシステムが現在接続されている無線ハブを介して送信される。この場合は、エンドシステムのホームネットワーク内のIWFが、アンカー、すなわちホームIWFとなる。こうしてエンドシステムとの間で授受されるPPPフレームは、無線ハブを介してホームネットワーク内のホームIWFに送られる。エンドシステムがホームに位置する場合、ホームIWFは無線ハブにXTunnelプロトコルを介して接続される。

【０２１４】フォーリンローミング無線サービスの場合（図２７）、フォーリン登録サーバは登録フェーズの際にローミングエンドシステムのホームネットワークの識別を見つける。この識別情報を用いて、フォーリン登録サーバはホーム登録サーバと通信し、エンドシステムの認証および登録を行なう。フォーリン登録サーバは、次に、サービングIWFを割り当て、ホームIWFとサービングIWFとの間にローミングエンドシステムのためにI-XTunnelプロトコル接続を確立する。サービングIWFは無線ハブとホームIWFとの間でフレームを中継する。ホームIWFからデータはPPPサーバ（つまり、ポイント・ツウ・ポイントプロトコルサーバ）に送られる。このPPPサーバは同一のIWF内に位置する場合もある。ただし、データが自身のPPPサーバを所有する企業イントラネットあるいはISPのイントラネットに向けられている場合は、データはL2TPプロトコルを介して別個のPPPサーバに送られる。この別個のサーバは、典型的には、無線サービスプロバイダとは別個のインターネットサービスプロバイダによって所有および運用される。ホームIWFとPPPサーバの位置はセッションを通じて固定されたままにとどまる。MAC層の登録とネットワーク層の登録を結合することで、MAC層の登録とネットワーク層の登録のために別個に要求されるオーバヘッドを節約することもできる。ただし、これら登録プロセスは結合しない方が、WSPの設備と純粋なIETF Mobile-IPをサポートする他の無線ネットワークとの相互運用性が確保でき便利である。

【０２１５】登録は、以下の３つのテーブルを設定する。テーブル１は、各アクセスポイントと関連する。テーブル１は各コネクション（例えば、各エンドシステム）をコネクションid（CID）にて識別し、コネクションidを特定の無線モデム（WM）のアドレス（つまり、エンドシステムのアドレス）と関連付ける。テーブル２は各無線ハブ（WH）と関連する。テーブル２は各コネクションidを対応する無線モデムアドレス、およびXTunnelのid（XID）と関連付ける。テーブル３は各インターワーキング機能（IWF）と関連する。テーブル３は各コネクションidを対応する無線モデムのアドレス、無線ハブのアドレス、XTunnelのid、およびIPポート（IP／ポート）と関連付ける。上述のテーブル内のエントリ（項目）は単にモビィリティ管理の説明に必要な項目のみを示し、実際には他にも重要なフィードが含まれることに注意する。

【０２１６】

【表１】

表１：ＡＰにおける接続テーブル

CID	WM
C1	WM1
C2	WM1
C1	WM2

表２：ＩＮＦにおける接続テーブル

CID	WM	AP	XID
C1	WM1	AP1	5
C2	WM1	AP1	5
C1	WM2	AP1	6
C1	WM3	AP2	7

表３：ＩＮＦにおける接続テーブル

CID	WM	WH	XID	IP/Port
C1	WM1	WH1	5	IP1/P1
C2	WM1	WH1	5	IP1/P2
C1	WM2	WH1	6	IP2/P3
C1	WM3	WH1	7	IP3/P1
C5	WM5	WH2	8	IP4/P1

【０２１７】図２８～３１は、ネットワーク内からダイアルフップするユーザ、並びに、ローミングユーザに対するプロトコルスタックを示す。図２８は、ホームの固定（つまり、移動しない）エンドシステムによる直接インターネットアクセスに対して用いるプロトコルスタックを示す。この構成では、PPPプロトコルメッセージはホームIWF（典型的には無線ハブと同一の位置に置かれる）に終端する。ホームIWFはメッセージをIPルータとの間で中継し、IPルータはメッセージをIWFと公衆インターネットの間で中継する。図２９は、ホームの固定（つまり、移動しない）エンドシステムによるリモートイントラネットアクセス（つまり、私設企業ネットあるいはISPへのアクセス）に対して用いるプロトコルスタックを示す。この構成では、PPPプロトコルメッセージはホームIWF（典型的には無線ハブと同一の位置に置かれる）を通じて私設企業イントラネットあるいはISPのPPPサーバに中継される。図３０は、フォーリンにローミングしているが固定の（つまり、移動していない）あるいは移動中のエンドシステムによる直接インターネットアクセスに対して用いられるプロトコルスタックを示す。この構成では、PPPプロトコルはホームIWF（典型的にはホームネットワークのモバイル交換センタ内に位置する）に終端し、ホームIWFは、IPルータとの間でメッセージを中継する。図３０に示すように、メッセージトラヒックはホームIWFに加えて、サービングIWF（典型的には無線ハブと同一の位置に置かれる）をも通ることに注意する。図３１は、フォーリンにローミングしているが固定の（つまり、移動していない）あるいは移動中のエンドシステムによるリモートイントラネットアクセス（つまり、私設企業ネットあるいはISPへのアクセス）に対して用いるプロトコルスタックを示す。この構成では、PPPプロトコルメッセージはホームIWF（典型的にはホームネットワークのモバイル交換センタ内に位置する）を通じて私設企業イントラネットあるいはISPのPPPサーバに中継される。図３１に示すようにメッセージトラヒックはホームIWFに加えて、サービングIWF（典型的には無線ハブと同一の位置に置かれる）をも通ることに注意する。サービングIWFと無線ハブがコンピュータの同一ネスト内に位置する場合、あるいは同一コンピュータ内にプログラムされている場合は、サービングIWFと無線ハブとの間にXTunnelプロトコルを用いてトンネルを設定する必要はない。

【０２１８】これらプロトコルスタックに対する同等な代替も可能である。例えば、RLPはサービングIWFあるいはホームIWF（モバイルがホームに位置する場合）に終端するのではなく、無線ハブに終端させることもできる。具体的には、IWFが無線ハブから遠く離れて位置し、パケットがIWFと無線ハブとの間の比較的損失が大きなIPネットワーク上を運ばれる場合は、RLPプロトコルは無線ハブの所に終端する方が好ましい。もう一つのバリエーションとしては、無線ハブとIWFの間のXtunnelは、必ずしもUDP/IPの上部に構築する必要がないことである。つまり、XtunnelはFrame Relay/ATM link層を用いて構築することもできる。ただし、UDP/IPを用いた方が、無線ハブおよびIWFソフトウエアをあるネットワークから別のネットワークに移動するのが楽になる。

【０２１９】４つのタイプのハンドオフシナリオが発生することが考えられ、これらは、それぞれ、（i）ローカルモビィリティ、（ii）マイクロモビィリティ、（iii）マクロモビィリティ、および（iv）グローバルモビィリティと呼ばれる。本発明の一つの実施例においては、これら４つの全てのシナリオにおいて、ルート最適化オプションは採用されず、ホーム登録サーバとISPのPPPサーバの位置は変更されない。ルート最適化を採用する本発明のもう一つの実施例においては、ISPのPPPサーバは変更されることがある。ただし、これについては後

に説明する。加えて、フォーリン登録サーバとIWFの位置も最初の３つのシナリオにおいては変更されない。

【０２２０】IETFが勧告するMobile IP標準は、エンドシステムがそれが接続されているIPサブネットを変更する場合は、必ず登録リクエストメッセージを自身のホームサブネット内のホームエージェントに送信することを要求する。このメッセージは新たなサブネット内でのエンドシステムとの連絡先である気付けアドレスを含む。トラヒックが、例えば、ISPからエンドシステムに向けて送信されると、ホームエージェントはこのエンドシステムに向けられたトラヒックを、これがホームサブネットに到着したとき傍受し、このトラヒックを気付けアドレスに転送する。この気付けアドレスはフォーリンサブネット内の特定のフォーリンエージェントを識別する。エンドシステムのフォーリンエージェントは、エンドシステム自身の中に駐在することも、トラヒックをエンドシステムに転送する別個のノード（つまり、代理登録エージェント）内に駐在することもある。Mobile IPのハンドオフにおいては、エンドシステムのエージェント、エンドシステムのホームエージェント、およびルート最適化オプションが採用される場合は対応するホスト（CH）の間で制御メッセージが交換される。

【０２２１】IETFが勧告するMobile IP標準では、大きなインターネット内の全ての移動に対して目標とされる遅延およびスケーラビリティを満足することは困難である。本発明の階層化されたモビィリティ管理ではこれら目標を満足することができる。小さな移動（例えばアクセスポイントの変更）の場合は、MAC-層の再登録のみが必要とされる。大きな移動の場合は、ネットワーク層の再登録が遂行される。本発明による階層化されたモビィリティ管理は、IETFによって勧告されるMobileIP標準において用いられるフラットな構造とも、（Cellular Digital Packet Data forumによってスポンサされる標準に基づく）CDPD等のセルラシステムにおいて用いられるサービング／アンカーインターワーキング機能とも異なる。

【０２２２】図３２に示すように、ローカルモビィリティハンドオフは、同一の無線ハブに属するAP間のエンドシステム（mobile nodeの略であるMNとして示す）の移動を扱う。このため、MAC層の再登録のみが必要となる。エンドシステムは、新たなAPから無線ハブアドバタイズメントを受信し、この新たなAPに向けて登録リクエストを送り返す。

【０２２３】この新たなAP（つまり、エンドシステムから登録リクエストを受信したAP）は、自身のコネクションテーブル内に新たなエントリを生成し、登録メッセージを自身の無線ハブに中継する。ローカルモビィリティハンドオフにおいては、無線ハブは変更されない。無線ハブは、エンドシステムの登録リクエストを、MACレベルの登録リクエストであるものと認識し、無線ハブは自身のコネクションテーブルをこの新たなAPを反映するように更新する。次に、以前のAPは、自身のコネクションテーブルから以前のコネクションエントリを削除する。以前のAPがエントリを以前のエントリを削除するためには、少なくとも次の３つの方法、つまり、（１）タイムアウトしたとき、（２）新たなAPから無線ハブに中継されたMAC層アソシエーションメッセージのコピーを受信したとき（この中継メッセージがブロードキャストメッセージである場合）、あるいは（３）無線ハブによるエントリを削除する旨の通知を受けたとき、に削除する方法がある。

【０２２４】図３３に示すように、マイクロモビィリティハンドオフは、同一の登録サーバに属する無線ハブ間のエンドシステム（mobile nodeの略であるMNとして示す）の移動で、かつ、エンドシステムが以前として現在のサービングIWFによって扱うことができる状況を扱う。アドバタイズメントが新たな無線ハブから（新たなAPを通じて）受信されると、エンドシステムは、その登録サーバへの登録をリクエストするメッセージを送信する。この登録リクエストは新たなAPと新たな無線ハブを通じてその登録サーバに中継される。

【０２２５】登録サーバは現在のIWFをまだ用いることができることを決定すると、登録サーバはbuild XTunnel Request message（XTunnel構築要請メッセージ）を現在のIWFに送ることで、現在のIWFに新たな無線ハブに向けてXTunnelを構築することを要請する。後に、登録サーバはtear down XTunnel Request message（XTunnel切断要請メッセージ）を現在のIWFに送ることで、現在のIWFに以前の無線ハブとの間の現在の XTunnelを切断することを要請する。このbuildおよびtear down XTunnel Request messageは一つのメッセージに結合することもできる。フォーリン登録サーバは、サービングIWFとホームIWFのいずれのIWFも変更されないために、登録メッセージをホーム登録サーバに転送することはない。

【０２２６】IWFからpositive build XTunnel reply（肯定的なXTunnel構築応答）およびpositive tear XTunnel reply（肯定的なXTunnel切断応答）を受信すると、登録サーバはエンドシステムに登録応答を送り返す。登録応答が新たな無線ハブに到着すると、新たな無線ハブの所のコネクションテーブルが新たなAPへの接続を反映するために更新される。新たなAPは、新たな無線ハブからメッセージが受信され、登録応答がエンドシステムに送り返された後に、自身のMACフィルタアドレステーブルおよびコネクションテーブルを更新する。

【０２２７】次に、登録サーバは、relese message（開放メッセージ）を以前の無線ハブに送信する。以前の無線ハブは、relese messageを受信すると、自身のコネクションテーブルとMACフィルタアドレステーブルおよび以前のAPのコネクションテーブルを更新する。

【０２２８】図３４に示すように、マクロモビィリティ

ハンドオフのケースは、フォーリンネットワーク内のサービングIWFは変更されるが、登録サーバは変更されない、無線ハブの間で移動を扱う。新たな無線ハブから（新たなAPを通じて）アドバタイズメントが受信されると、エンドシステムはネットワーク層の登録をリクエストするメッセージを登録サーバに向けて送信する。この登録リクエストは、新たなAPと新たな無線ハブを経て登録サーバに中継される。

【０２２９】登録サーバは、エンドシステムが現在の登録サーバのネットワークに属さない場合、自身がフォーリン登録サーバであると認識する。フォーリン登録サーバは、リクエスト、好ましくは、Radius Accessリクエスト（RAリクエスト）をフォーリンダイレクトリサーバ（大きなイエローページに類似）に送信することで、ホーム登録サーバの識別を見つけ、次に、適当なIWFをサービングIWFとして割り当て、その後、登録リクエスト、好ましくは、Radius Accessリクエスト（RAリクエスト）をホーム登録サー バに送信することで、ホーム登録サーバに新たに選択されたIWFを通知する。

【０２３０】ホーム登録サーバは、リクエスト、好ましくは、Radius Accessリクエスト（RAリクエスト）をホームダイレクトリサーバに送ることで、登録リクエストを認証（検証）する。登録リクエストが認証され、さらに、現在のホームIWFはまだ用いることができることが決定されると、ホーム登録サーバは、ホームIWFに対して、新たに割り当てられたサービングIWFに向けて新たなI-XTunnelを構築することと、以前のサービングIWFへの現在のI-XTunnelを切断することを指令する。ホームIWFからpositive buidld I-XTunnel replay（肯定的なI-XTunnel構築応答）およびpositive tear I-XTunnel reply（肯定的なI-XTunnel切断応答）を受信すると、ホーム登録サーバは、フォーリン登録サーバに登録応答を送り返す。

【０２３１】すると、フォーリン登録サーバは、新たに割り当てられたIWFに対して、新たな無線ハブに向けてXTunnelを構築することを指示する。positive buidld I-XTunnel replayを受信すると、フォーリン登録サーバは以前のIWFに対して、以前の無線ハブへのXTunnelを切断することを指令する。positive buidld I-XTunnel replayおよびpositive tear I-XTunnel replyを受信すると、フォーリン登録サーバはエンドシステムに登録応答を返信する。

【０２３２】登録応答が新たな無線ハブに到着すると、新たな無線ハブの所のコネクションテーブルが新たなAPへの接続を反映するように更新される。新たなAPは、新たな無線ハブからメッセージが受信され、登録応答がエンドシステムに送り返された後に、自身のMACフィルタアドレステーブルおよびコネクションテーブルを更新する。

【０２３３】次に、登録サーバはrelease message（開放メッセージ）を以前の無線ハブに送信する。無線ハブがrelease messageを受信すると、これは、自身のコネクションテーブルおよびMACフィルタアドレステーブルを更新し、以前のAPは、以前の無線ハブからメッセージを受信した後に自身のMACフィルタアドレステーブルおよびコネクションテーブルを更新する。

【０２３４】グローバルモビィリティハンドオフのケースは、登録サーバの変更を伴う無線ハブの間の移動を扱う。図３５はホームIWFは変更されない場合のグローバルモビィリティハンドオフを示し、図３６はホームIWFも変更される場合のグローバルモビィリティハンドオフを示す。新たなフォーリンネットワーク内の新たな無線ハブから（新たなAPを通じて）アドバタイズメントを受信すると、エンドシステムはネットワーク層の登録をリクエストするメッセージを新たなフォーリン登録サーバに送る。この登録リクエストは新たなAPと新たな無線ハブを経て新たなフォーリン登録サーバに中継される。

【０２３５】登録サーバは、エンドシステムが現在の登録サーバのネットワークに属さない場合、自身がフォーリン登録サーバであると認識する。フォーリン登録サーバは、リクエスト、好ましくは、Radius Accessリクエスト（RAリクエスト）をフォーリンダイレクトリサーバ（大きなイエローページに類似）に送信することで、ホーム登録サーバの識別を見つけ、次に、適当なIWFをサービングIWFとして割り当て、その後、登録リクエスト、好ましくは、Radius Accessリクエスト（RAリクエスト）をホーム登録サーバに送ることで、ホーム登録サーバに新たに選択されたIWFを通知する。

【０２３６】ホーム登録サーバは、リクエスト、好ましくは、Radius Accessリクエスト（RAリクエスト）をホームダイレクトリサーバに送ることで、登録リクエストを認証（検証）する。リクエストが認証され、現在のホームIWFをまだ用いることができることを決定すると（図３５）、ホーム登録サーバは、ホームIWFに対して、新たなフォーリン登録サーバによって新たに割り当てられたサービングIWFに向けて新たなI-XTunnelを構築することを指令する。ホーム登録サーバは、さらに、以前のフォーリン登録サーバにde-registration message（登録解消メッセージ）を送信するとともに、ホームIWFに対して、以前のフォーリンネットワークの以前のサービングIWFへの以前のI-XTunnelを切断することを指令する。ホームIWFからpositive buidld I-XTunnel replay（肯 定的なI-XTunnel構築応答）およびpositive tear I-XTunnel reply（肯定的なI-XTunnel切断応答）を受信すると、ホーム登録サーバはregistration reply（登録応答）を新たなフォーリン登録サーバに送る。

【０２３７】次に、新たなフォーリン登録サーバは、新たに割り当てられたIWFに対して、新たな無線ハブに向けてXTunnelを構築することを指令する。positive buidld XTunnel replay（肯定的なXTunnel構築応答）を受信

すると、フォーリン登録サーバはエンドシステムに向けて登録応答を送り返す。この登録応答が新たな無線ハブに到着すると、新たな無線ハブの所のコネクションテーブルが新たなAPへの接続を反映するように更新される。新たなAPは、自身のMACフィルタアドレステーブルおよびコネクションテーブルを、新たな無線ハブからメッセージが受信され、登録応答がエンドシステムに転送された後に更新する。

【０２３８】次に、以前のフォーリン登録サーバは、以前のIWFに対して、以前の無線ハブへのXTunnelを切断するように指令する。positive tear XTunnel reply（肯定的なXTunnel切断応答）を受信すると、あるいはtear down XTunnel request（XTunnel切断リクエスト）を送信するのと同時に、以前のフォーリン登録サーバは、以前の無線ハブにrelease message（開放メッセージ）を送信する。以前の無線ハブがrelease messageを受信すると、これは、自身のコネクションテーブルおよびMACフィルタアドレステーブルを更新し、以前のAPは、自身のMACフィルタアドレステーブルおよびコネクションテーブルを以前の無線ハブからメッセージを受信した後に更新する。

【０２３９】他方、図３６に示すように、ホーム登録サーバが新たなフォーリン登録サーバからの登録リクエストは認証されたが、以前のホームIWFは用いることができないことが決定された場合は、ホーム登録サーバは新たなホームIWFを選択し、新たなホームIWFに対して、現在のPPPサーバ（例えば、接続されたISPイントラネット内のPPPサーバ）に向けて、レベル２トンネルプロトコルによるトンネル（つまりL2TPトンネル）を構築することを指令する。次に、ホーム登録サーバは、以前のホームIWFに対して、そのL2TPトンネルトラヒックを新たなホームIWFに転送することを指令する。

【０２４０】次に、ホーム登録サーバは、新たなホームIWFに対して、新たなフォーリン登録サーバによって新たに割り当てられたサービングIWFに向けて新たなI-XTunnelを構築することを指令する。ホーム登録サーバは、さらに、de-registration message（登録解消メッセージ）を以前のフォーリン登録サーバに送信するとともに、ホームIWFに対して、以前のフォーリンネットワークの以前のサービングIWFへの以前のI-XTunnelを切断することを指令する。ホームIWFからpositive buidld I-XTunnel replay（肯定的なI-XTunnel構築応答）およびpositive tear I-XTunnel reply（肯定的なI-XTunnel切断応答）を受信すると、ホーム登録サーバは登録応答を新たなフォーリン登録サーバに送信する。

【０２４１】すると、新たなフォーリン登録サーバは、新たに割り当てられたIWFに対して、新たな無線ハブへのXTunnelを構築することを指令する。positive build XTunnel replay（肯定的なXTunnel構築応答）を受信すると、フォーリン登録サーバはエンドシステムに向けて登録応答を送り返す。登録応答が新たな無線ハブに到着すると、無線ハブの所のコネクションテーブルが新たなAPへの接続を反映するように更新される。新たなAPは、自身のMACフィルタアドレステーブルおよびコネクションテーブルを、新たな無線ハブからメッセージが受信され、登録応答がエンドシステムに転送された後に更新する。

【０２４２】以前のフォーリン登録サーバは、以前のIWFに対して、以前の無線ハブへのXTunnelを切断することを指令する。positive tear XTunnel reply（肯定的なXTunnel切断応答）を受信するとあるいはtear down XTunnel reques（XTunnel切断要請）を送信するのと同時に、以前のフォーリン登録サーバはrelease message（開放メッセ ージ）以前の無線ハブに送信する。以前の無線ハブは開放メッセージを受信すると、自身のコネクションテーブルおよびMACフィルタアドレステーブルを更新し、以前のAPは、自身のMACフィルタアドレステーブルおよびコネクションテーブルを以前の無線ハブからメッセージを受信した後に更新する。

【０２４３】本発明に従って構成されたエンドシステムはIETFが勧告するMobile-IP標準に従って構成されたネットワークと相互に動作でき、IETFが勧告するMobile-IP標準に従って構成されたエンドシステムも本発明に従って構成されたネットワークと相互に動作できる。

【０２４４】本発明のネットワークとIETF Mobile-IP（rfc2002、標準ドキュメント）との主な差異は以下の通りである：

（i）本発明がモビィリティ管理のために階層概念を用いるのに対して、IETFが勧告するMobile-IP標準は、フラットな構造を用いる。本発明のネットワークにおいては、小さなエリア内での小さなモビィリティ（ハンドオフ）に対しては、ネットワークレベルの登録は必要とされない。マイクロモビィリティは、新たなXtunnelの設定と以前のXtunnelの切断を伴う。グローバルモビィリティは、最小でも、XTunnelの設定／切断に加えて、新たなI-XTunnelの設定と以前のI-XTunnelの切断を伴う。グローバルモビィリティは、新たなL2TP Tunnelの設定および以前のL2TP Tunnelから新たなL2TP TunnelへのL2TP状態の転送を伴う。

【０２４５】（ii）本発明は、リモートダイヤルアップユーザを識別するために、ユーザ名＋領域（realm）を用いるにの対して、IETFが勧告するMobile-IP標準は固定ホームアドレスを用いる。

（iii）本発明では登録機能とルーティング機能は別個のエンティティによって遂行される。これら２つの機能はIETFが勧告するMobile-IP標準ではホームエージェントによって遂行され、両方の機能はIETFが勧告するMobile-IP標準ではフォーリンエージェントによっても遂行される。これにと対象的に、本発明の一つの実施例においては、登録機能は登録サーバによって遂行され、ルー

ティング機能は、ホームIWFとフォーリンIWFの両方および無線ハブ（アクセスハブとも呼ばれる）によって遂行される。

【０２４６】（iv）本発明は、PPPセッション当たり３つのトンネルを用いる。XTunnelは、無線ハブとサービングIWFとの間のlink-layer tunnel（リンク層トンネル）により近い。サービングIWFとホームIWFとの間のI-XTunnelは、IETFが勧告するMobile-IP標準のホームとフォーリンエージェントとの間のトンネルにより近い。ただし、これは、Mobile-IP標準によって勧告されるトンネルを超える追加の機能を持つ。L2TPトンネルはホームIWFがPPPサーバでない場合にのみ用いられる。これらトンネルの数は、前述のように、幾つかの機能を同一ノードに併合することで削減することができる。

【０２４７】（v）本発明では、ネットワーク層の登録はPPPセッションが開始される前に発生するのに対して、IETFが勧告するMobile-IP標準では、Mobile-IPの登録は、PPPセッションがオープン状態に入った後に発生する。

（vi）本発明では、エージェントアドバタイズメントをアドバタイズするネットワークエンティティ（つまり、無線ハブ）は、エンドシステムへの直接リンク上には存在しないのに対して、IETFが勧告するMobile-IP標準では、エージェントアドバタイズメントは、TTL of １（１のTTL）を持つことが要求され、これはエンドシステムがフォーリンエージェントと直接リンクを持つことを意味する。加えて、本発明のエージェントアドバタイズメントは、IETFが勧告するMobile-IP標準の場合のようなICMPルータアドバタイズメントに対する拡張ではない。

【０２４８】本発明によるエンドシステムはエージェント請求（agent solicitation）をサポートすることを要求される。本発明によるエンドシステムが、IETFが勧告するMobile-IP標準をサポートするネットワークを訪問した場合、エンドシステムはエージェントアドバタイズメントが送られているのを待つ（聞こえるのを待つ）。もし、エンドシステムが、エージェントアドバタイズメントを妥当な時間フレーム内に受信しない場合、エンドシステムはエージェント請求（agent solicitation）をブロードキャストする。

【０２４９】本発明においては、ネットワーク運用者は、IETFが勧告するMobile-IP標準をサポートする他のネットワークと、それら他のネットワークを用いることを希望する本発明によるエンドシステムにホームアドレスを割り当てられるように協議することができる。本発明のエンドシステムは、エージェントアドバタイズメントを受信したとき、それが訪問しているネットワークが本発明によるネットワークではないことを決定し、登録のためにこうして割り当てられたホームアドレスを用いることができる。

【０２５０】IETFが勧告するMobile-IP標準をサポートするネットワークの場合は、PPPセッションが、Mobile-IPの登録の前に開始され、PPPサーバはそれらのネットワーク内のフォーリンエージェントと同一の位置にあるものと想定される。一つの実施例においては、SNAPヘッダを用いてPPPフレームが本発明のMACフレームに（Ethernetフォーマットと類似する方法にて）カプセル化され、フォーリンエージェントはこのフォーマットをproprietary PPP format over Ehthernet encapsulationであると解釈する。こうして、本発明によるエンドシステムと相手のPPPはオープン状態に入ることができる。その後、フォーリンエージェントは、エージェントアドバタイズメントの送信を開始し、本発明のエンドシステムは登録が可能となる。

【０２５１】IETFが勧告するMobile-IP標準をサポートするエンドシステムが本発明のタイプのネットワーク内で動作できるようにするためには、これらモバイル（エンドシステム）は少なくとも類似のMAC層の登録を遂行できることが必要とされる。本発明のエージェントアドバタイズメントメッセージのフォーマットをIETFが勧告するMobile-IP標準のエージェントアドバタイズメントメッセージのフォーマットと類似させることで、本発明のネットワークに訪問するエンドシステムは、エージェントアドバタイズメントを解釈し、無線ハブに登録することが可能となる。本発明の登録リクエストおよび応答メッセージは、IETFが勧告するMobile-IP標準の登録リクエストおよび応答メッセージに（不要な拡張なしに）類似し、このため、本発明のモビィリティ管理機能の他の部分は、本発明のネットワークに訪問するエンドシステムに透過的である。

【０２５２】IETFが提唱するMobile-IP標準をサポートするエンドシステムはMobile-IP登録の前にPPPセッションが開始されることを期待するために、本発明の無線ハブは、オプションとして、MAC-層の登録の後にPPPのLCP（Link control Protocok）パケットおよびNCP（Network Control Protocol）パケットの解釈を開始することもできる。ハンドオフの際にトラヒックが失われるのを回避するために、本発明のモビィリティ管理は、メークビフォアブレーク（make before break）という概念を用いる。ローカルモビィリティの場合は、メークビフォアブレークコネクション（make before break connection）は、新たなAPによって無線ハブに中継されるMAC-層登録メッセージをブロードキャスメッセージに変換することによって達成される。こうして、以前のAPは、新たな登録を聞くことができ、エンドシステムに向けられたまだ伝送されてないパケットを新たなAPに転送することが可能となる。

【０２５３】マイクロモビィリティの場合は、新たな無線バブに関する情報がサービングIWFと以前の無線ハブとの間で交換されるTear XTunnelメッセージ内に挿入される。こうして、以前の無線ハブは、サービングIWFか

らのTear XTunnelメッセージを聞いたときに、緩衝したパケットを新たな無線ハブに転送することが可能となる。同時に、WIFの所のRLP層がそれまでに以前の無線ハブから確認応答のあったシーケンス番号を覚えている。同時に、IWFも、以前の無線ハブに送られた最も新しいパケットの現在の送信シーケンス番号（current send sequence number）を覚えている。こうして、IWFは、これら２つの番号の間に来るパケットを、新たな無線ハブに、より新たなパケットを新たな無線ハブに送信する前に送信することが可能となる。RLP層は重複パケットをフィルタできるものと想定される。第二のアプローチの方が、以前の無線ハブは互いに直接に通信できないと考えられるために、第一のアプローチよりも好ましい。

【０２５４】マクロモビィリティの場合は、以前の無線ハブから新たな無線ハブへのパケット転送に加えて、以前のサービングIWFがパケットを新たなサービングIWFに転送する。これを達成するためには、単に、新たなサービングIWFの識別をtear down1-XTunnelメッセージに挿入して新たなサービングIWFに送ることのみが必要とされる。これと同一の結果を達成するためのもう一つの方法として、ホームIWFは、以前のサービングIWFによって最後に確認応答のあったI-XTunnelのシーケンス番号と、ホームIWFによって送信された現在のI-XTunnelのシーケンス番号を知っているために、以前のサービングIWFが損失パケットを新たなサービングIWFに転送するのでなくホームIWFがこの仕事を遂行する方法である。

【０２５５】ハンドオフの間でのトラヒック損失を最小にするためにどれだけの量のバッファを、それぞれ、モバイル当たり／AP当たり／無線ハブ当たり／IWF当たりに割り当てるかを推定する一つの方法としては、エンドシステム当たり／AP当たり／無線ハブ当たり／IWF当たりのパケット到着速度とハンドオフ時間を推定する方法がある。この情報をIWFの無線ハブの以前のAPにパスすることで、ハンドオフ時に、それぞれ、IWFの無線ハブの新たなAPにどの程度のトラヒックが転送されるべきか決定される。

【０２５６】本発明においてルートの最適化を達成するためには、エンドシステムはサービングIWFに最も近いPPPサーバを選択する。ルート最適化なしでは、過剰な輸送遅延や過剰な物理リンクの使用が発生することがある。例えば、ニューヨーク市内のホームネットワークに加入するエンドシステムが香港にローミングするものと想定する。香港のISPにリンクを設定するためには、エンドシステムは、香港内の無線ハブ内に設定されたサービングIWFと、ニューヨーク市内のホームネットワーク内に設定されたホームIWFとを持つこととなる。この場合、メッセージは、（香港にローミングした）エンドシステムから（香港内の）サービングIWFに向かい、ここから（ニューヨーク市内の）ホームIWFを経て、再び、香港のISPに戻るようにルートされる。

【０２５７】一つの好ましいアプローチは（香港内の）サービングIWFを直接に香港のISPに接続する方法である。この場合は、サービングIWFがホームIWFのように機能する。この実施例においては、前提として、ホームとフォーリン無線プロバイダの間にローミング合意が存在する。加えて、課金情報が共有されるようにさまざまなアカウンティング／課金システムが互いに自動的に通信するようにされる。アカウンティングおよび課金情報の交換はIETFのROAMOPS作業グループによって勧告される標準等を用いて実現する。

【０２５８】ただし、サービングIWFは、この場合でも、最も近いPPPサーバ（例えば、香港のISP）を見つけることを必要とされる。現在の実施例においては、フォーリン登録サーバはエンドシステムのPPPサーバ（例えば、香港のISP）への接続の希望をフォーリン登録サーバがエンドシステムから登録リクエストを受信したときに知る。フォーリン登録サーバがサービングIWFの方が要求されるPPPサーバ（例えば、香港のISP）にホームIWFよりも近いことを知ると、フォーリン登録サーバはサービングIWFに対して、L2TPトンネルを（ホーム登録サーバおよびホームIWFに最も近いPPPサーバではなく）自身に最も近いPPPサーバに向けて確立することを指令する。次に、フォーリン登録サーバは、ホーム登録サーバにエンドシステムがサービングIWFとフォーリンPPPによるサービスを受けている事実を通知する。

【０２５９】もう一つの実施例においては、フォーリン登録サーバはサービングIWFの方が希望されるPPPサーバ（例えば、香港のISP）にホームIWFより近いことを、フォーリン登録サーバがエンドシステムから登録リクエストを受信したときに知る。すると、フォーリン登録サーバは登録リクエストメッセージにサービングIWFの情報を示すメッセージとルート最適化が要望されることを示す通知とを付加して、これをホーム登録サーバに送る。同時にフォーリン登録サーバはサービングIWFに対して、L2TPトンネルをPPPサーバに向けて確立することを指令する。登録リクエストが承認された時点で、ホーム登録サーバはホームIWFに対してL2TPの状態をフォーリンIWFに転送するように指令する。

【０２６０】無線エンドユーザがローミングできる新規のネットワークアーキテクチャの幾つかの好ましい実施例について説明したが、これらは単に説明を意図するもので、制限を加えることを意図するものではなく、当業者においては上述の教示に照らして様々な修正およびバリエーションを考えることができると思われる。例えば、ここで説明された接続リンクには、周知の接続プロトコル（例えば、IP、TCP/IP、L2TP、IEEE 802.3等）を用いて設定されるが；ただし、本発明から逸脱することなく、他の接続プロトコルを用いて同一あるいは類似のデータ配信能力を持つ接続リンクを設定することも可能である。上述の様々な実施例における動作エージェント

(acting agent) は、ソフトウエアによって制御されるプロセッサの形式を取ることも、他の制御の形式（例えば、プログラマブル論理アレイ等）を取ることもできる。動作エージェントは説明のようにグループ化することも、あるいは、説明の接続方法から逸脱することなく、上述のセキュリティおよび認証方法を達成できることを条件に、別の仕方にグループ化することもできる。さらに、単一の、アクセスポイント、アクセスハブ（つまり無線ハブ）あるいはインターワーキング機能ユニット（IWFユニット）にて、マルチチャネル能力を提供することもできる。このため、単一の、アクセスポイント、アクセスハブあるいはIWFユニットにて複数のエンドシステムからのトラヒッを扱うこともでき、従って、ここでは別個の複数の、アクセスポイント、アクセスハブあるいはIWFユニットとして説明されたものと同一なものを、単一のマルチチャネル、アクセスポイント、アクセスハブあるいはIWFにて実現することもできる。従って、開示された本発明の幾つかの特定な実施例に対して、特許請求の範囲によって定義される本発明の範囲および精神から逸脱することなく、様々な変更を加えることができるものである。

【図面の簡単な説明】

【図１】公衆交換電話ネットワークを通じての周知のリモートアクセスアーキテクチャの構成図である。

【図２】本発明による無線パケット交換データネットワークを通じてのリモートアクセスアーキテクチャの構成図である。

【図３】本発明の一つの実施例によるエンドシステムの構成を示す。

【図４】本発明の一つの実施例によるエンドシステムのもう一つのエンドシステムの構成を示す。

【図５】本発明の一つの実施例によるエンドシステムのさらにもう一つのエンドシステムの構成を示す。

【図６】図２のネットワークのアーキテクチャのローミングシナリオを示す選択された部分の構成図である。

【図７】ローカルアクセスポイントを持つ基地局の構成図である。

【図８】リモートアクセスポイントを持つ基地局の構成図である。

【図９】リモートアクセスポイントを持つ基地局であって、幾つかのリモートアクセスポイントが無線トランク接続を用いて接続される構成図である。

【図１０】ローカルアクセスポイントに対するプロトコルスタックの図である。

【図１１】無線トランクを持つリモートアクセスポイントに対するプロトコルスタックの図である。

【図１２】リモートアクセスポイントを無線トランクにてサポートするための基地局内の中継機能に対するプロトコルスタックの図である。

【図１３】図１２に示す中継機能を実現するためのプロトコルスタックの図である。

【図１４】ローカルアクセスポイントをサポートするための基地局内の中継機能に対するプロトコルスタックの図である。

【図１５】図２のネットワークのアーキテクチャの選択された部分の構成図であって、ホームネットワークからホームネットワークに登録する第一のエンドシステムと、フォーリンネットワークからホームネットワークにホームインターワーキング機能をアンカーとして用いて登録する第二のエンドシステムを示す。

【図１６】図２のネットワークのアーキテクチャの選択された部分の構成図であって、ホームネットワークからホームネットワークに登録する第一のエンドシステムと、フォーリンネットワークからホームネットワークにサービングインターワーキング機能をアンカーとして用いて登録する第二のエンドシステムを示す。

【図１７】フォーリンネットワークからホームネットワークに登録するため、および、データリンクを、確立、認証、および構成するために用いるリクエストおよび応答メッセージの梯子図である。

【図１８】図２のネットワークのアーキテクチャの選択された部分の構成図であって、モバイルをホームネットワークからホームネットワークに登録する際の登録リクエストおよび応答を示す。

【図１９】図２のネットワークのアーキテクチャの選択された部分の構成図であって、モバイルをフォーリンネットワークからホームネットワークに登録する際の登録リクエストおよび応答を示す。

【図２０】ホームネットワーク内のエンドシステムとホームネットワーク内のインターワーキング機能との間の通信であって、セルサイトがローカルアクセスポイントを持つ場合のプロトコルスタックの構成図である。

【図２１】ホームネットワーク内のエンドシステムとホームネットワーク内のインターワーキング機能との間の通信であって、セルサイトが無線トランクを通じて無線ハブに接続されたリモートアクセスポイントを持つ場合のプロトコルコルスタックの構成図である。

【図２２】ローミングエンドポイントに結合された基地局とホームインターワーキング機能との間の通信を示すプロトコルスタックの構成図である。

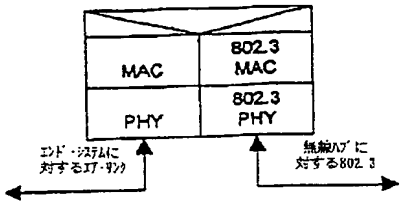
【図2,3】ホームネットワーク内のエンドシステムがホームネットワーク内のインターワーキング機能を通じてインターネットプロトコルプロバイダに接続する場合の通信を示すプロトコルスタックの構成図である。

【図２４】フォーリンネットワーク内のエンドシステムとホームネットワーク内のホーム登録サーバとの間の登録フェーズの際の通信を示すプロトコルスタックの構成図である。

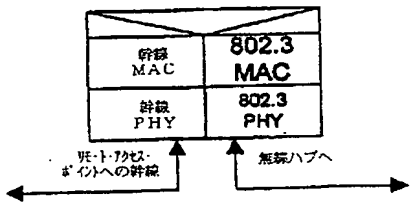
【図２５】アカウンティングデータを顧客課金システムに送るまでの処理を示す処理流れ図である。

【図２６】ホームネットワーク内のエンドシステムに対する登録プロセスを示す梯子図である。
【図２７】フォーリンネットワーク内のエンドシステムに対する登録プロセスを示す梯子図である。
【図２８】PPPプロトコルがホームネットワークのインターワーキングに終端する場合のホームネットワーク内のエンドシステムの接続を示すプロトコルスタック図である。
【図２９】PPPプロトコルがISPあるいはイントラネットに終端する場合のホームネットワーク内のエンドシステムの接続を示すプロトコルスタック図である。
【図３０】PPPプロトコルがフォーリンネットワークのインターワーキング機能に終端する場合のフォーリンネットワーク内のエンドシステムの接続を示すプロトコルスタック図である。
【図３１】PPPプロトコルがISPあるいはイントラネットに終端する場合のフォーリンネットワーク内のエンドシステムの接続を示すプロトコルスタック図である。
【図３２】ローカルハンドオフシナリオを示す梯子図である。
【図３３】マイクロハンドオフシナリオを示す梯子図である。
【図３４】マクロハンドオフシナリオを示す梯子図である。
【図３５】グローバルハンドオフシナリオであって、フォーリン登録サーバは変更されるが、ホームインターワーキング機能は変更されない場合を示す梯子図である。
【図３６】グローバルハンドオフシナリオであって、フォーリン登録サーバとホームインターワーキング機能の両方が変更される場合を示す梯子図である。
【図３７】可能な接続を示すシステムの構成図である。
【図３８】可能な接続を示すシステムの構成図である。
【図３９】様々なハンドオフシナリオを示す。
【図４０】様々なハンドオフシナリオを示す。
【図４１】様々なハンドオフシナリオを示す。
【図４２】様々なハンドオフシナリオを示す。
【符号の説明】
４　ユーザモデム
２　ユーザコンピュータ
８　ポイントオブプレゼンス（POP）
１０　イントラネットバックボーン
１４　メディアデータセンタ
１２　ルータ
１８　プライベートイントラネット
２０　公衆インターネットバックボーン
２１　アンテナ
２２　RFケーブル
２３　ラジオ
２４　デスクトップコンピュータ
２６　マルチツイステッドペアケーブル
２７　壁変圧器
２８　無線LAN
２９　アンテナ
３０　無線ネットワーク
３２　エンドシステム
３４　エアリンク
３６　基地局
３８　バックホールネットワーク
４０　モバイル交換センタ（MSC）
４２　IPルータ
４４　公衆インターネット
４６　プライベートイントラネット
４６　インターネットサービスプロバイダ
４８　アカウンティングおよびディレクトリサーバ
５０　要素管理サーバ
５２　パケットデータインタワーキング機能（IWF）
６０　ローミングエンドシステム
６２　フォーリン無線サービスプロバイダ
６４　基地局
６６　サービングIWF
７０　ホーム無線サービスプロバイダ
７２　ホームIWF
７４　インターネットサービスプロバイダ
８０　無線サブネットワーク
８２　アクセスポイント
８４　無線ハブ
８６　無線トランク

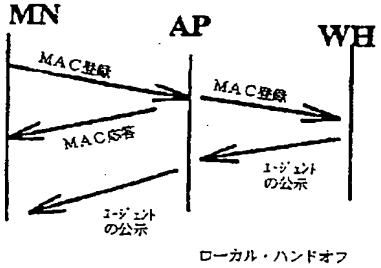
【図１０】



【図１１】

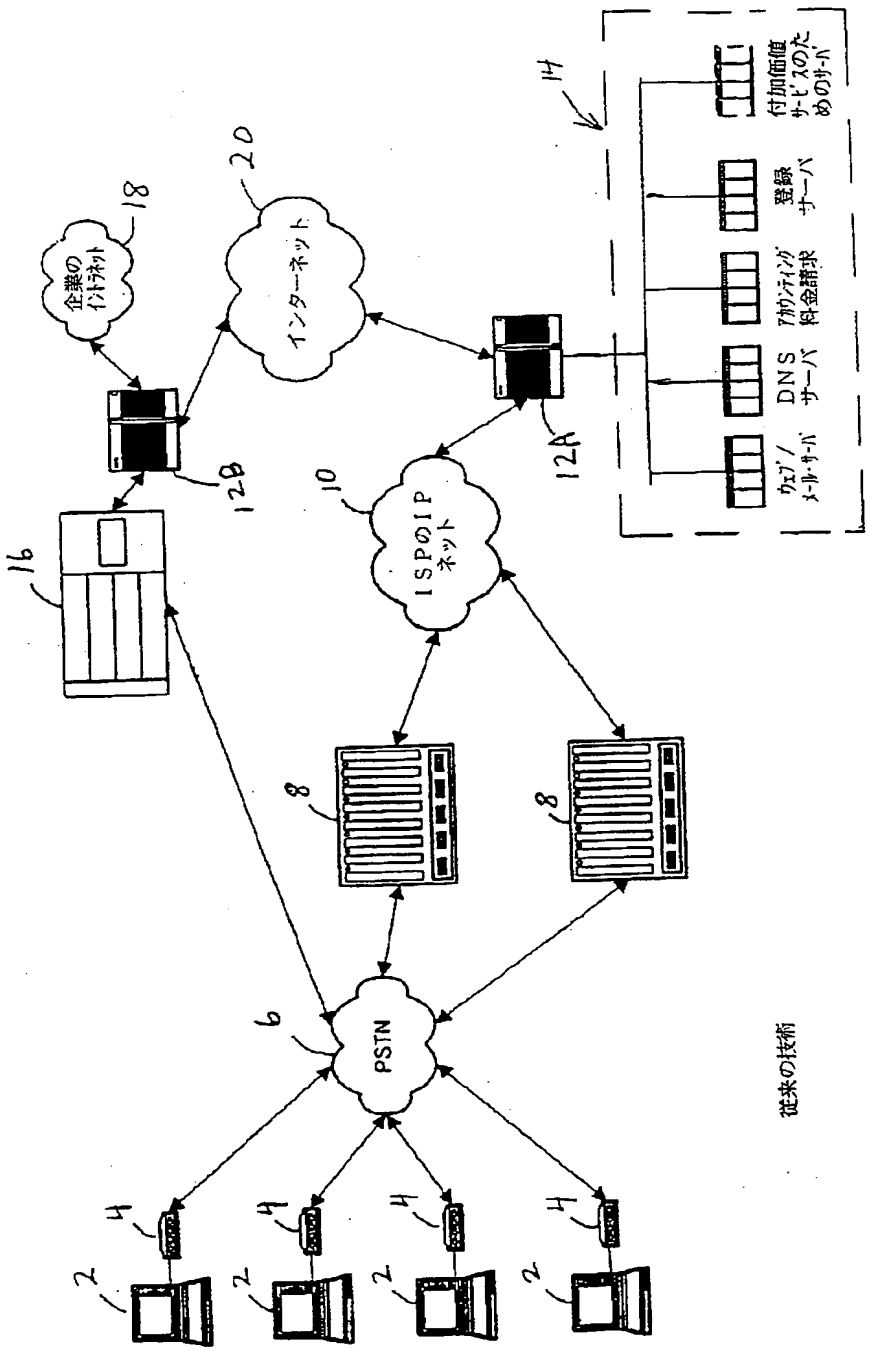


【図３２】

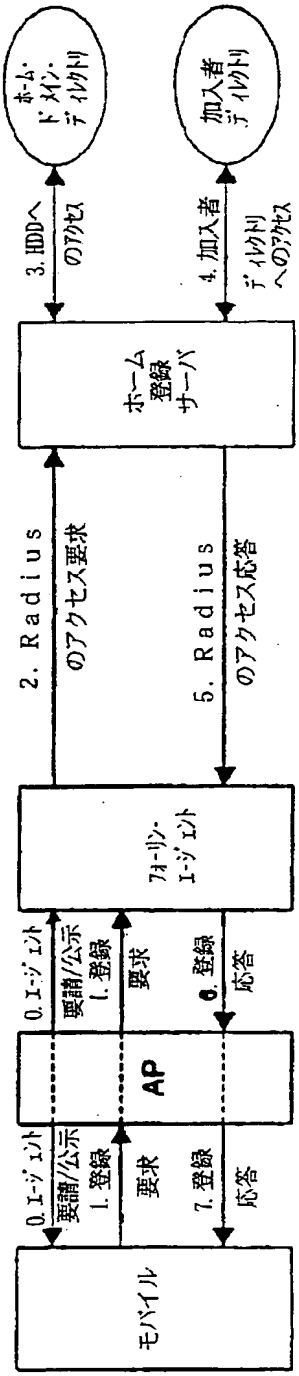


ローカル・ハンドオフ

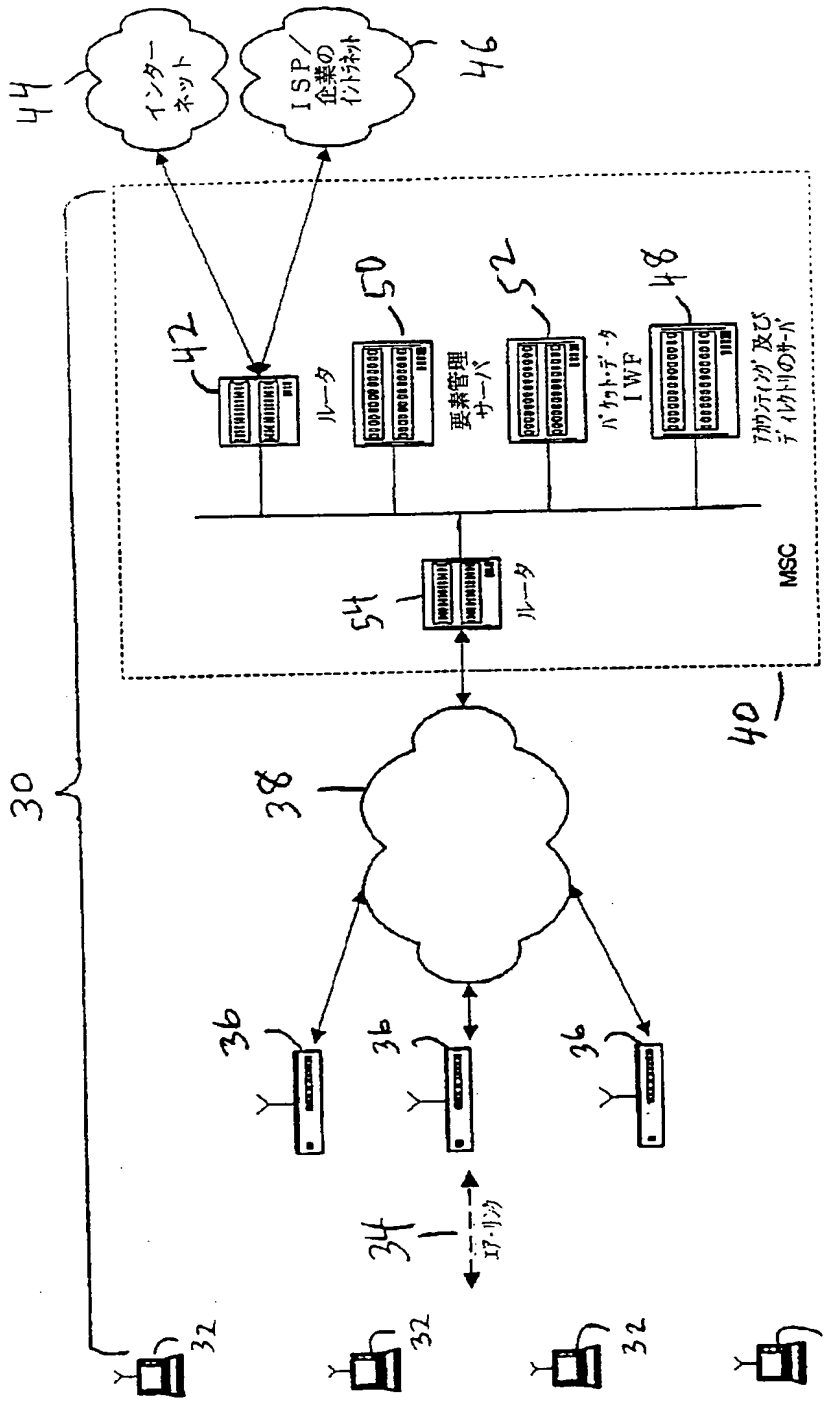
【図１】


企業のイントラネット
18
インターネット
20
14
付加価値サービスのためのサーバ
登録サーバ
アカウンティング料金請求
DNSサーバ
ウェブ／メール・サーバ
12B
12A
16
10
ISPのIPネット
8
8
PSTN
6
4
4
4
4
2
2
2
2
ホーム無線サービス・プロバイダ
従来の技術

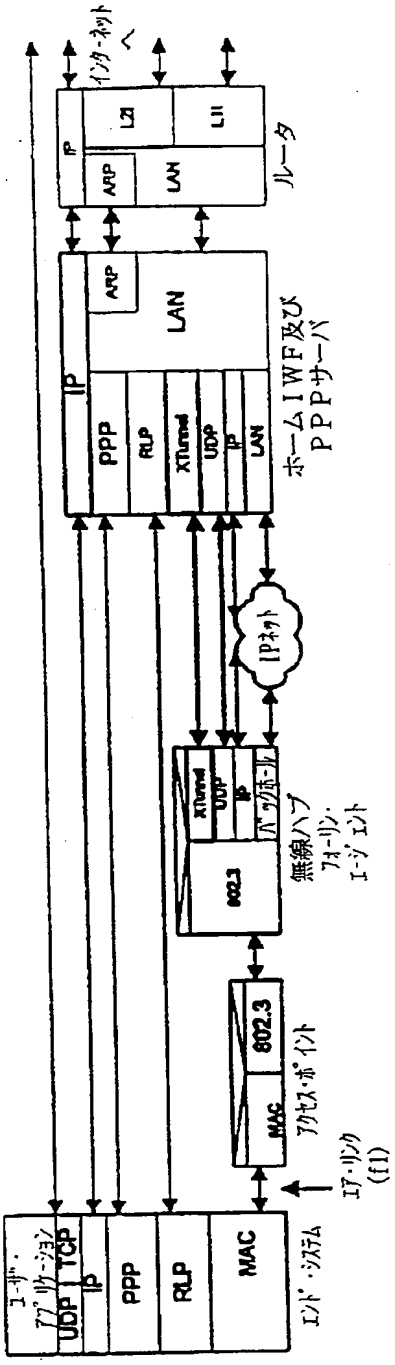
【図１８】


ホーム・ドメイン・ディレクトリ
加入者ディレクトリ
3. HDDへのアクセス
4. 加入者ディレクトリへのアクセス
2. Radiusのアクセス要求
5. Radiusのアクセス応答
ホーム登録サーバ
フォーリン・エージェント
AP
モバイル
0. エージェント要請/公示
1. 登録要求
6. 登録応答
7. 登録応答

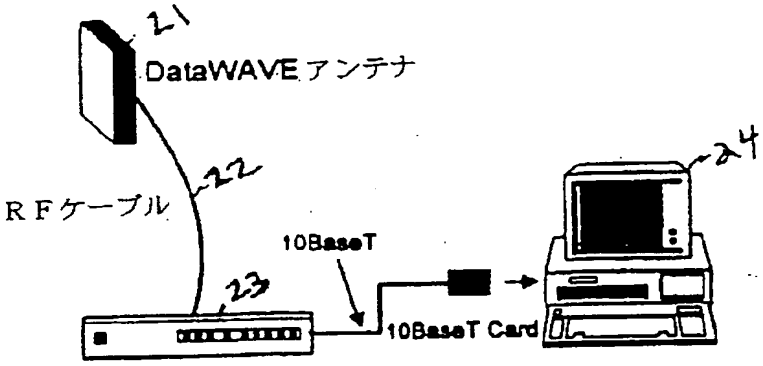
【図２】


44
インター
ネット
ISP/
企業の
イントラネット
46
42
ルータ
50
要素管理
サーバ
52
パケット・データ
IWF
48
アカウンティング及び
ディレクトリのサーバ
54
ルータ
MSC
40
30
38
36
36
36
34
IP・リンク
32
32
32
32

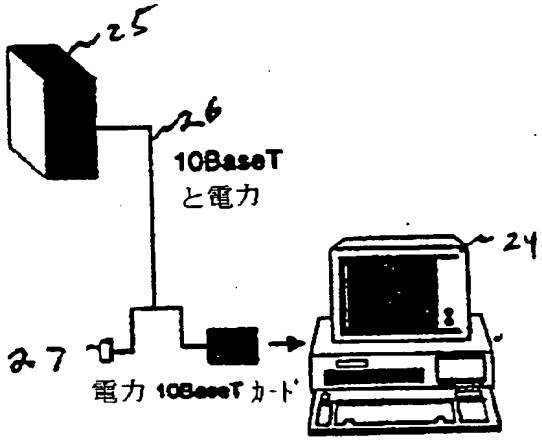
【図２０】


インター・ネットへ
IP
LCI
LLI
ARP
LAN
ルータ
ARP
LAN
IP
PPP
RLP
XTunnel
UDP
IP
LAN
ホームIWF及び
PPPサーバ
IPネット
XTunnel
UDP
IP
802.3
無線ハブ
802.3
MAC
アクセス・ポイント
IP・リンク
(f1)
ユーザ・
アプリケーション
UDP TCP
IP
PPP
RLP
MAC
エンド・システム

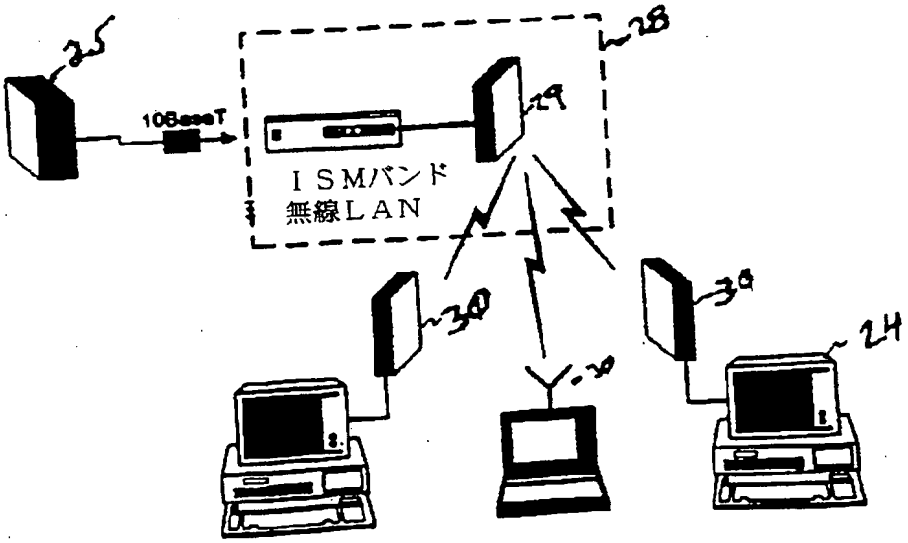
【図３】



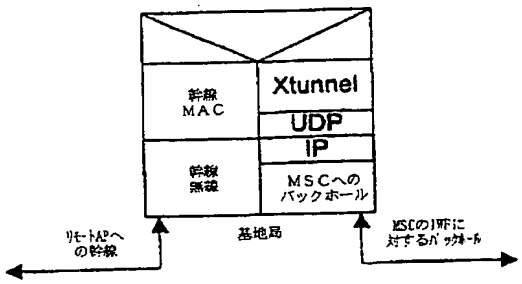
【図４】



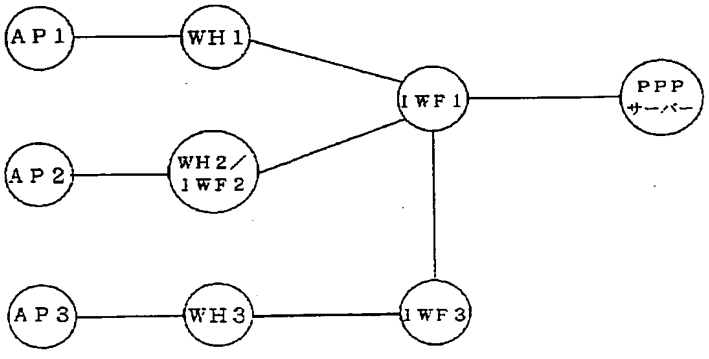
【図５】



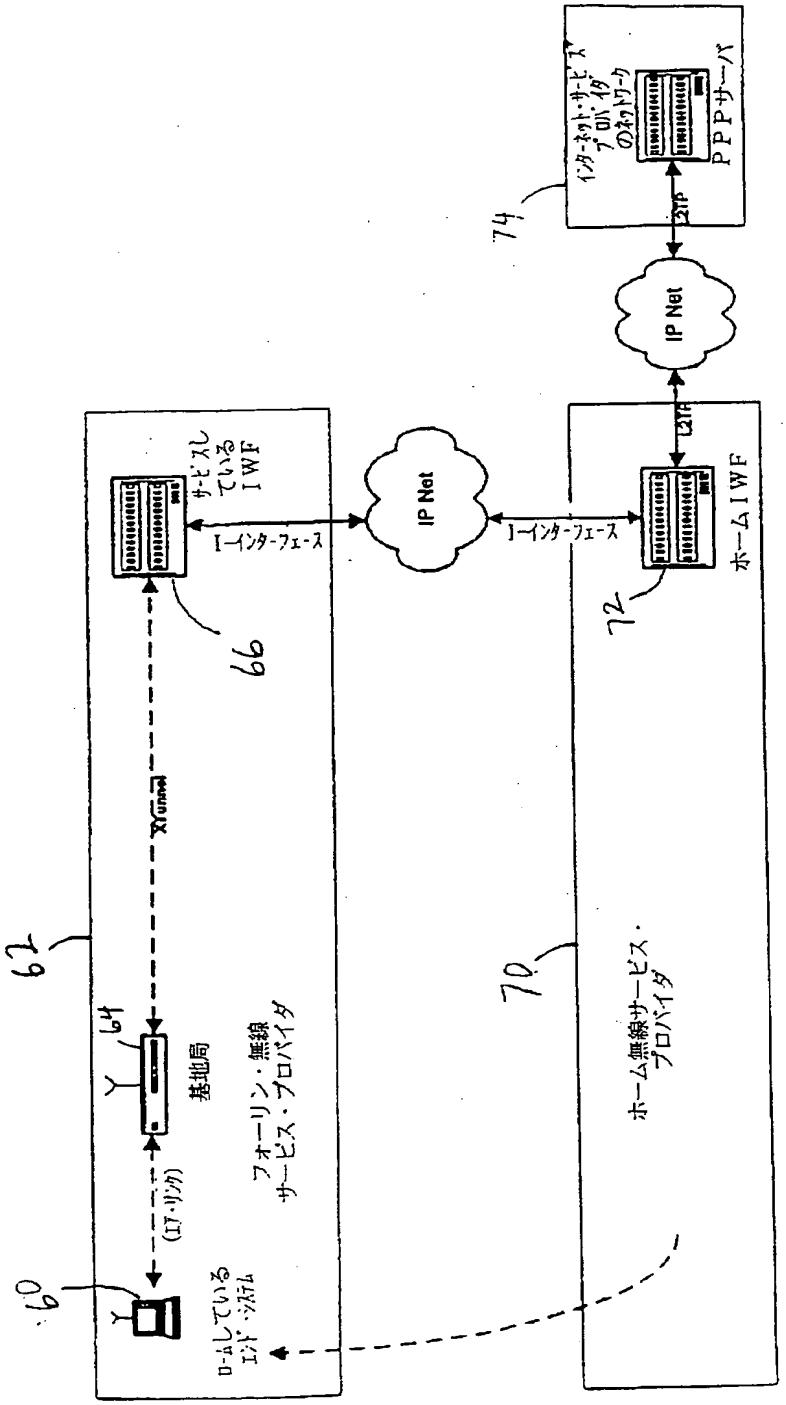
【図１２】



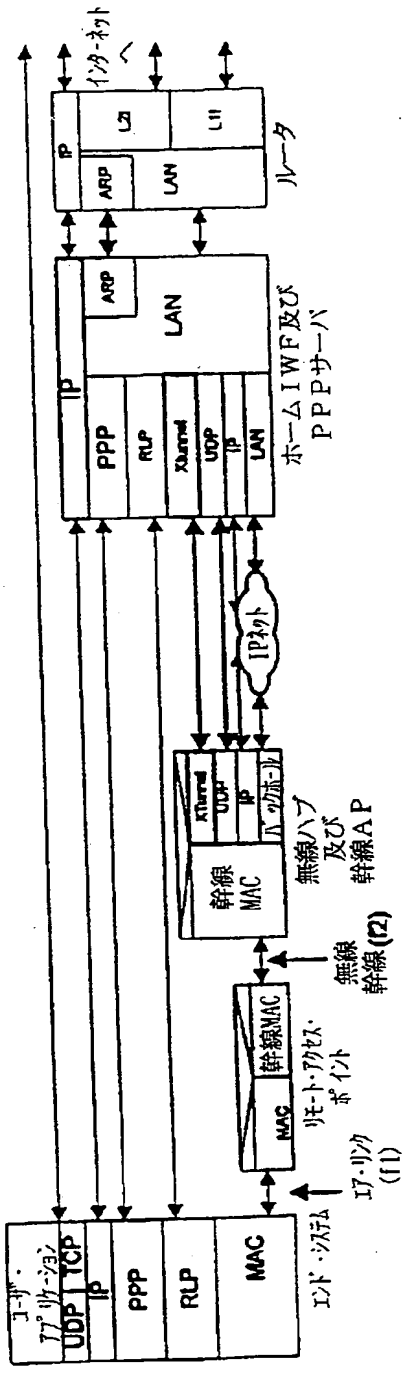
【図３７】



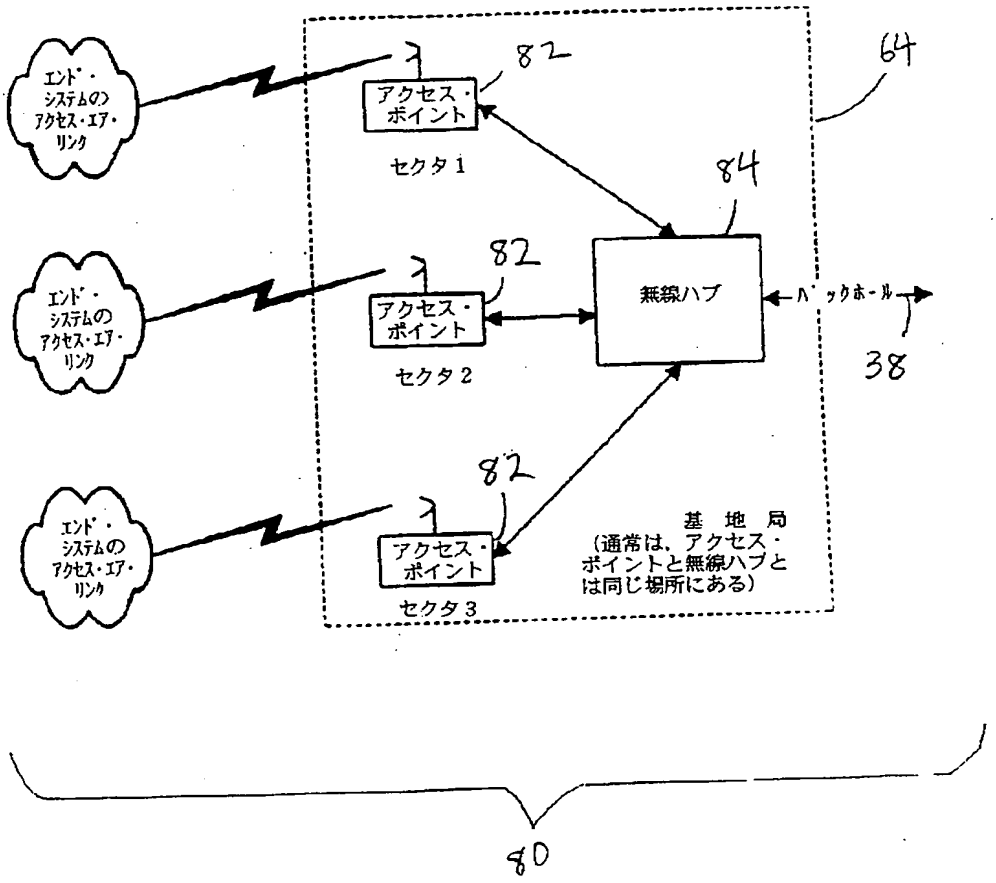
【図６】


62
60
64
66
70
72
74
基地局
フォーリン・無線
サービス・プロバイダ
ホーム無線サービス・
プロバイダ
ホームIWF
IP Net
PPPサーバ
インターネット・サービス
プロバイダのネットワーク
Xtunnel
L2TP
L1
(エア・リンク)

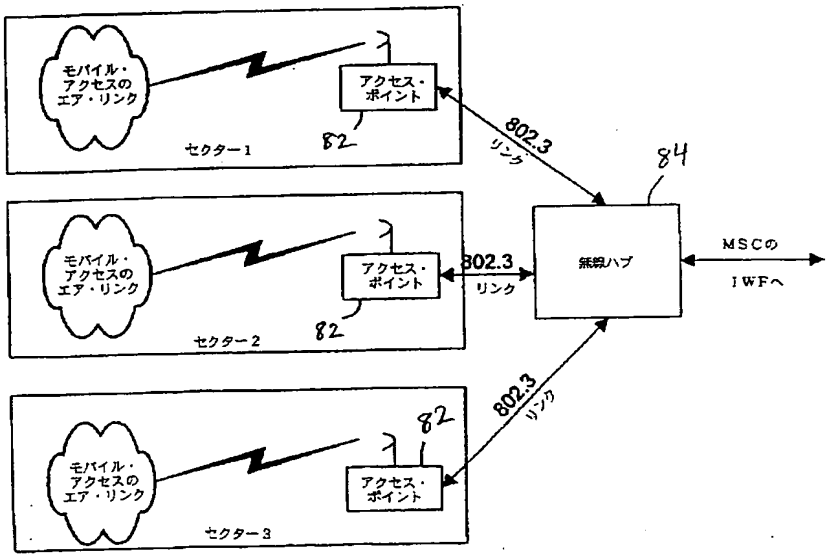
【図２１】


インターネットへ
ルータ
IP
ARP
LAN
L3
L2
L1
ホームIWF及び
PPPサーバ
PPP
RLP
Xtunnel
UDP
IPネット
無線ハブ
及び
幹線AP
幹線MAC
無線
幹線(I2)
リモート・アクセス・
ポイント
エア・リンク
(I1)
エンド・システム
アプリケーション
TCP
MAC

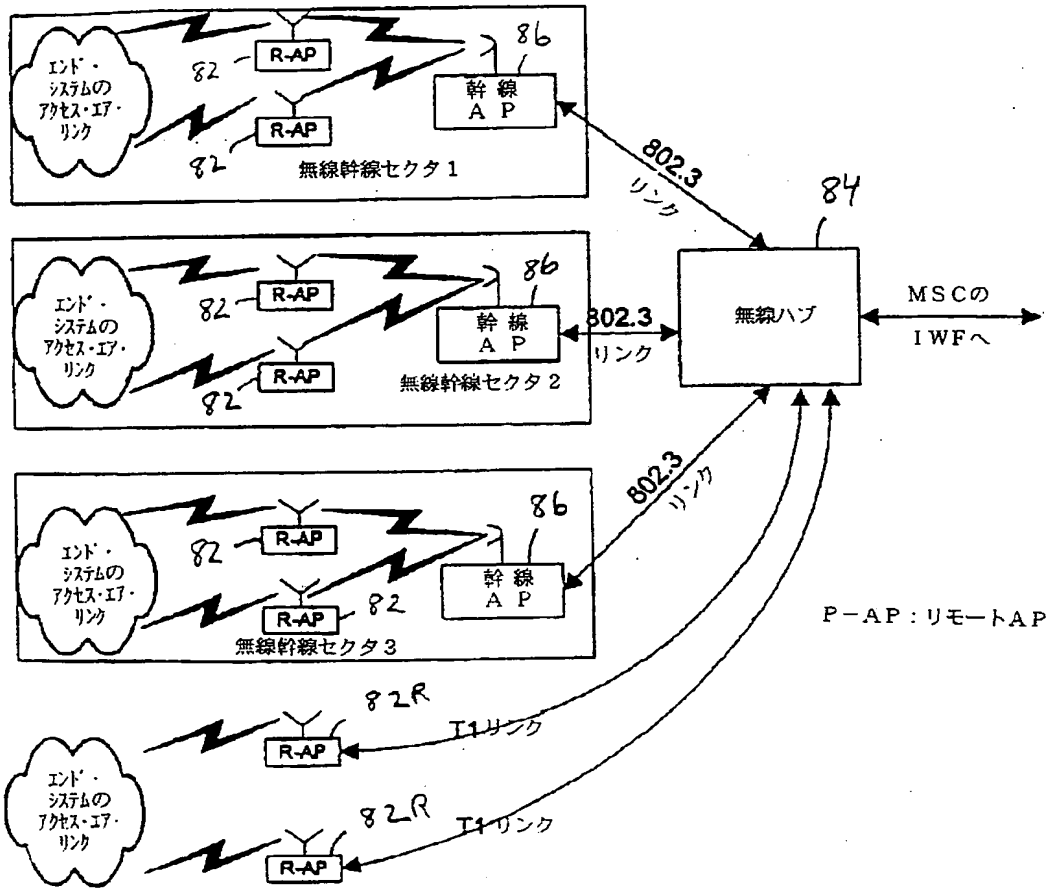
【図７】


エンド・システムのアクセス・エア・リンク
アクセス・ポイント
82
セクタ１
64
84
無線ハブ
バックホール
38
セクタ２
セクタ３
基地局
（通常は、アクセス・ポイントと無線ハブとは同じ場所にある）
80

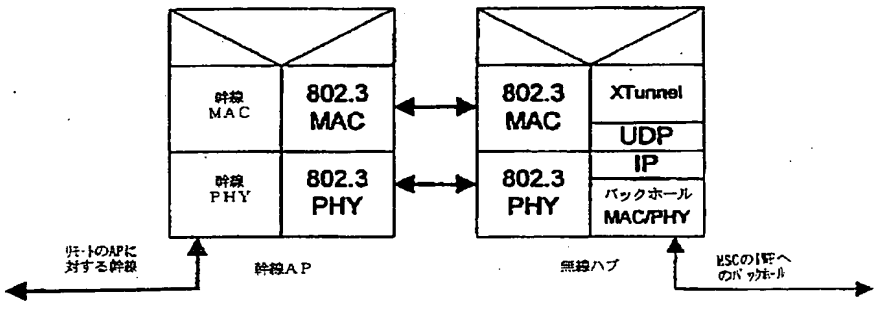
【図８】


モバイル・アクセスのエア・リンク
アクセス・ポイント
82
セクター１
802.3 リンク
84
無線ハブ
MSCの IWFへ
セクター２
セクター３

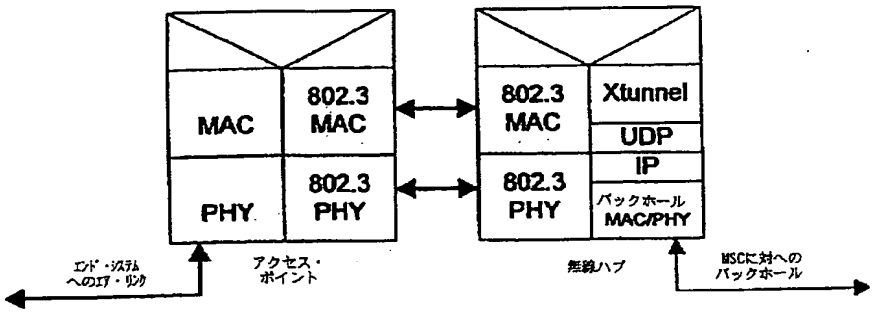
【図９】


エンド・システムのアクセス・エア・リンク
R-AP
82
86
幹線AP
802.3リンク
84
無線幹線セクタ１
無線幹線セクタ２
無線幹線セクタ３
無線ハブ
MSCのIWFへ
P－AP：リモートAP
82R
I1リンク

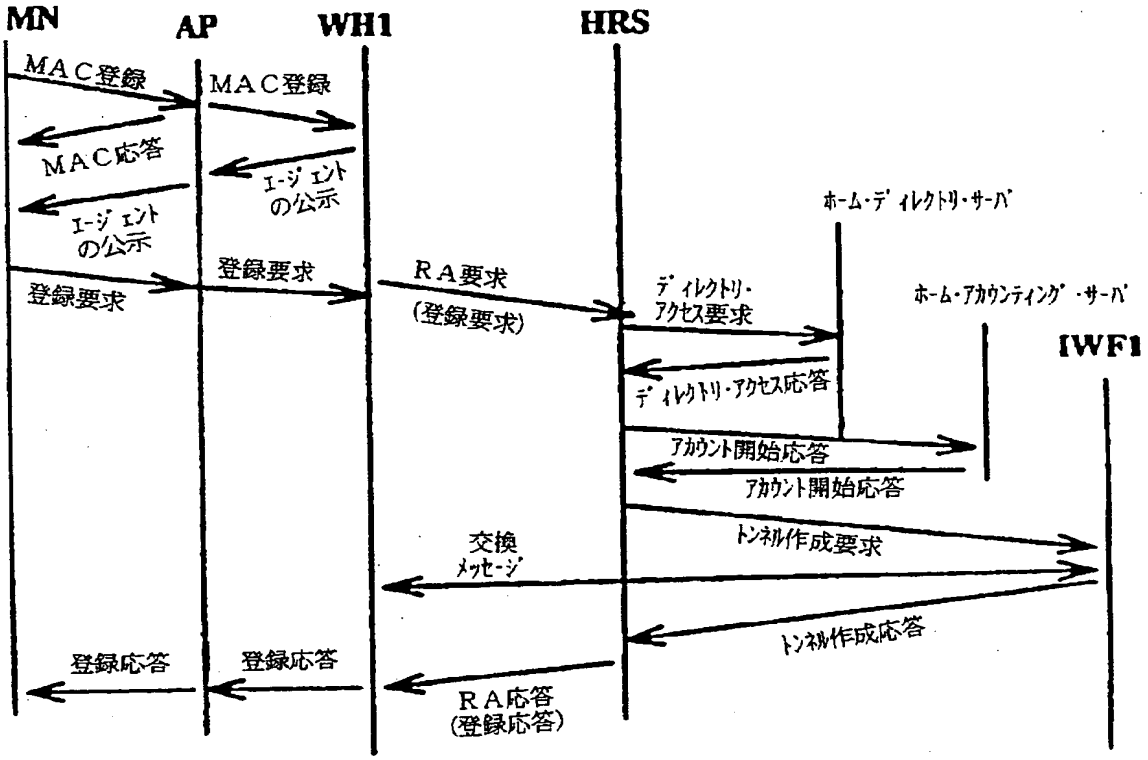
【図１３】


幹線MAC
802.3 MAC
幹線PHY
802.3 PHY
802.3 MAC
802.3 PHY
XTunnel
UDP
IP
バックホールMAC/PHY
幹線AP
無線ハブ

【図１４】

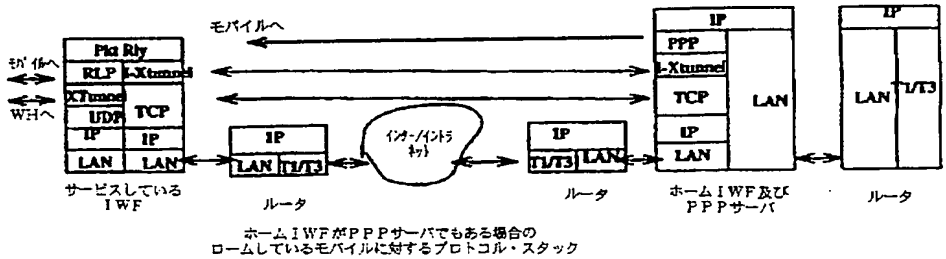


【図２６】



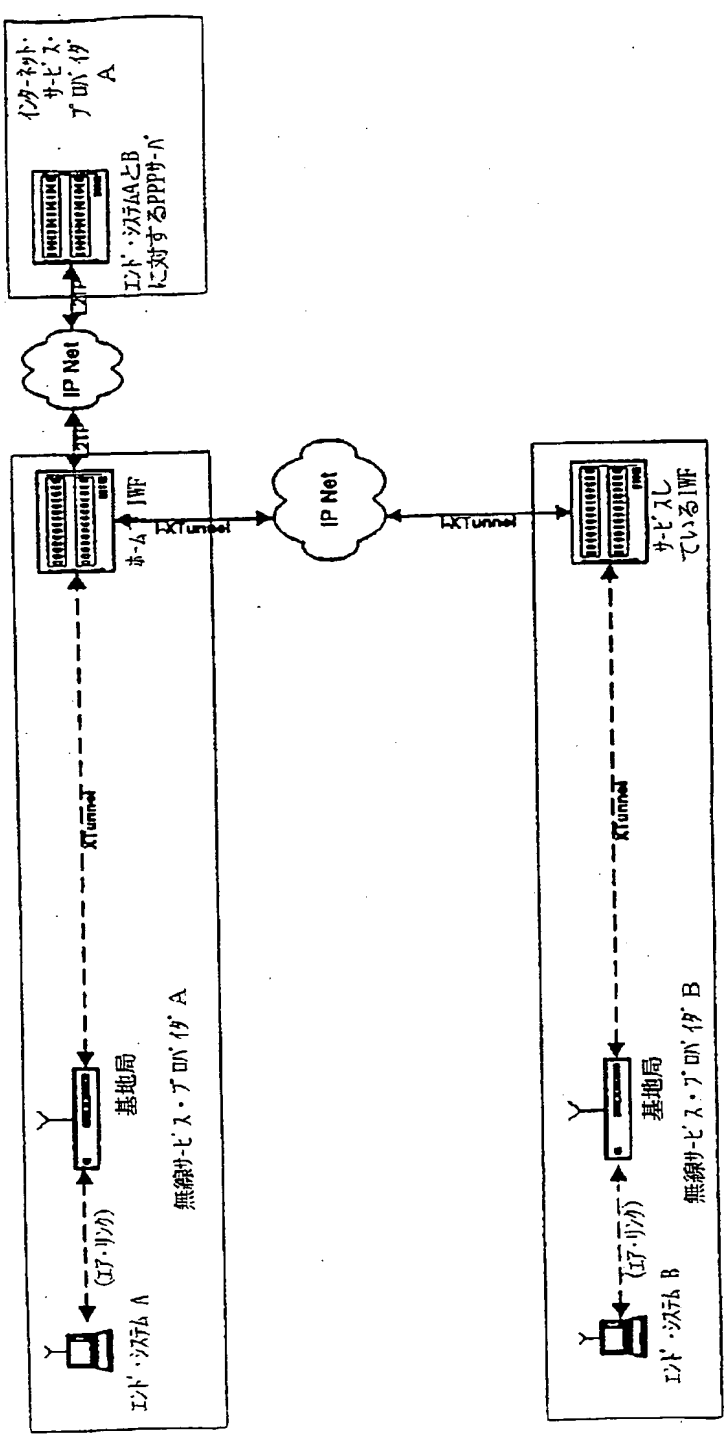
ホームにおける登録

【図３０】

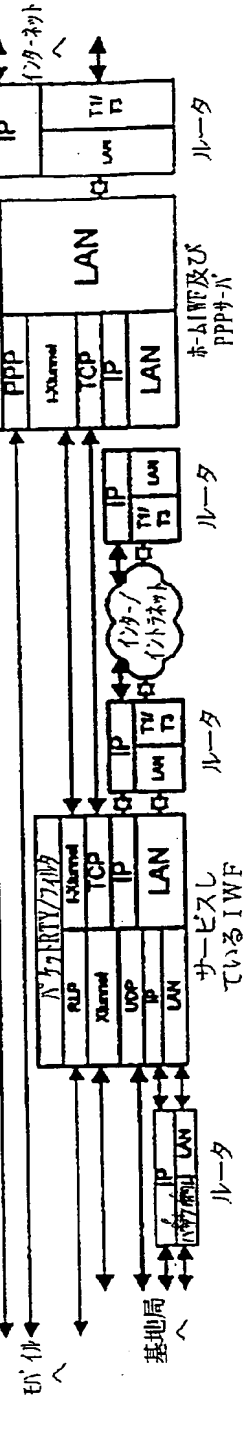


ホームＩＷＦがＰＰＰサーバでもある場合の
ローミングしているモバイルに対するプロトコル・スタック

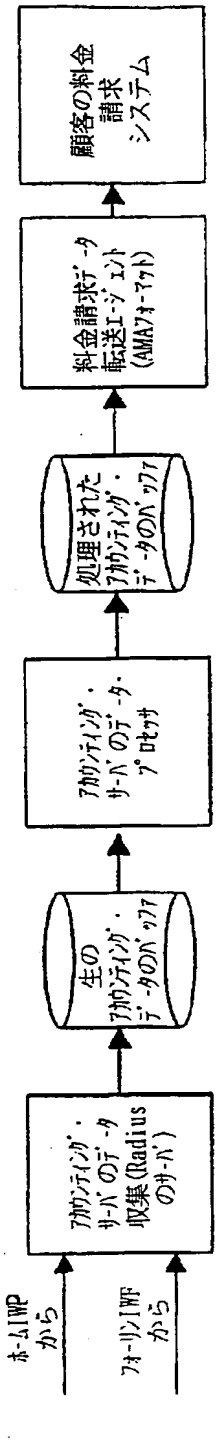
【図１５】


インターネット・サービス・プロバイダA
エンド・システムAAとBに対するPPPサーバ
IP Net
IWF
ホームA
XTunnel
IP Net
XTunnel
サービスしているIWF
基地局
無線サービス・プロバイダA
エンド・システムA
(エア・リンク)
基地局
無線サービス・プロバイダB
エンド・システムB
(エア・リンク)

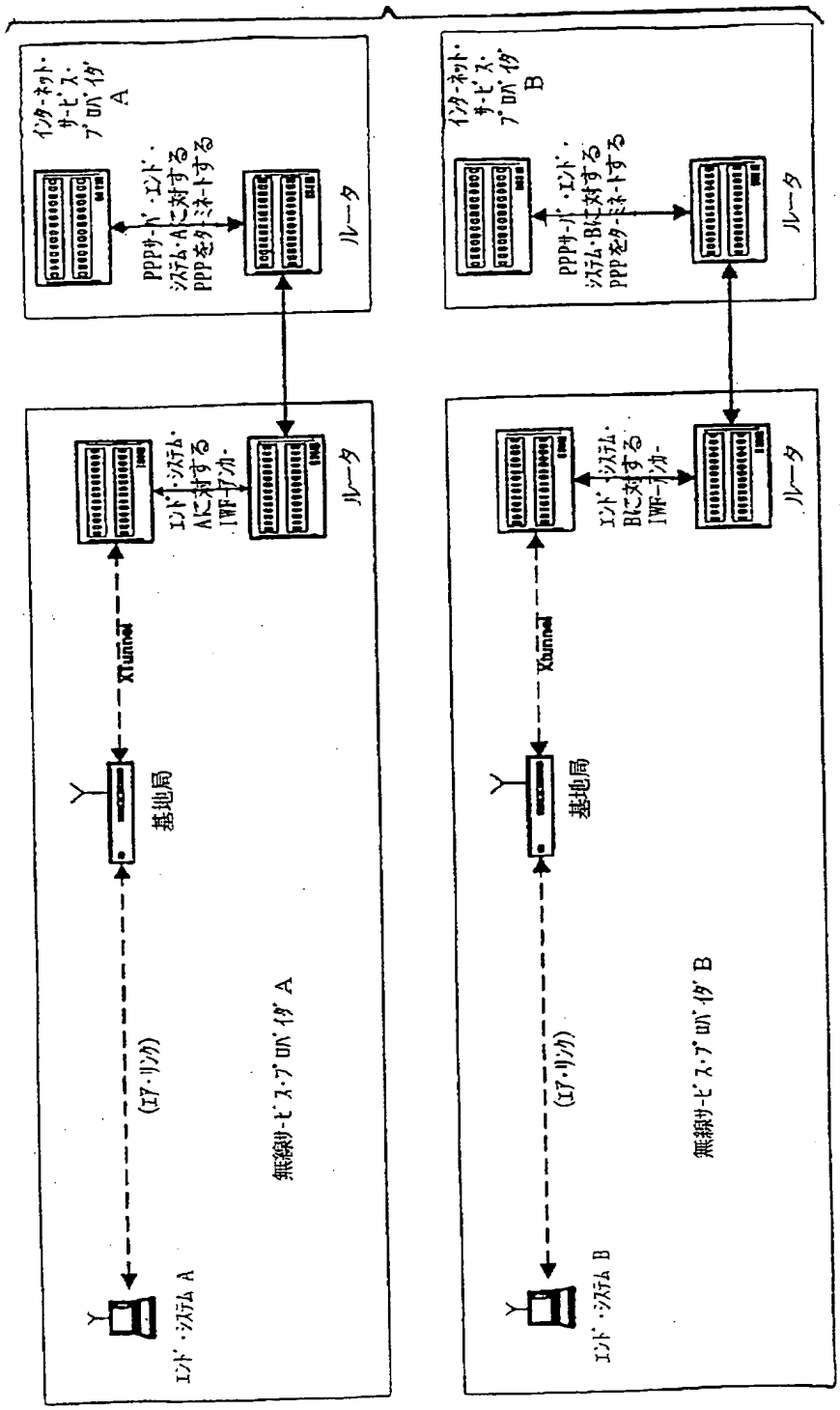
【図２２】


インターネットへ
IP
ルータ
LAN
PPP
TCP
IP
ホームIWF及びPPPサーバ
ルータ
インターノイントラネット
ルータ
ルータ
ケーブルTVプロバイダ
サービスしているIWF
ISP
へ
基地局
へ

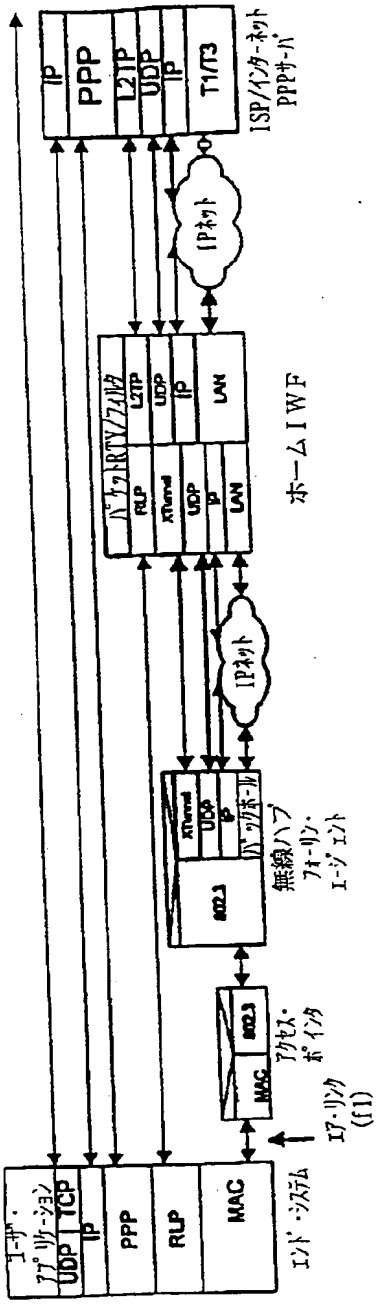
【図２５】


顧客の料金請求システム
料金請求データ転送エージェント(AMAソフトウェア)
処理されたアカウンティング・データのバッファ
アカウンティング・サーバのデータ・プロセッサ
生のアカウンティング・データのバッファ
アカウンティング・サーバのデータ収集(Radiusのサーバ)
ホームIWPから
フォーリンIWFから

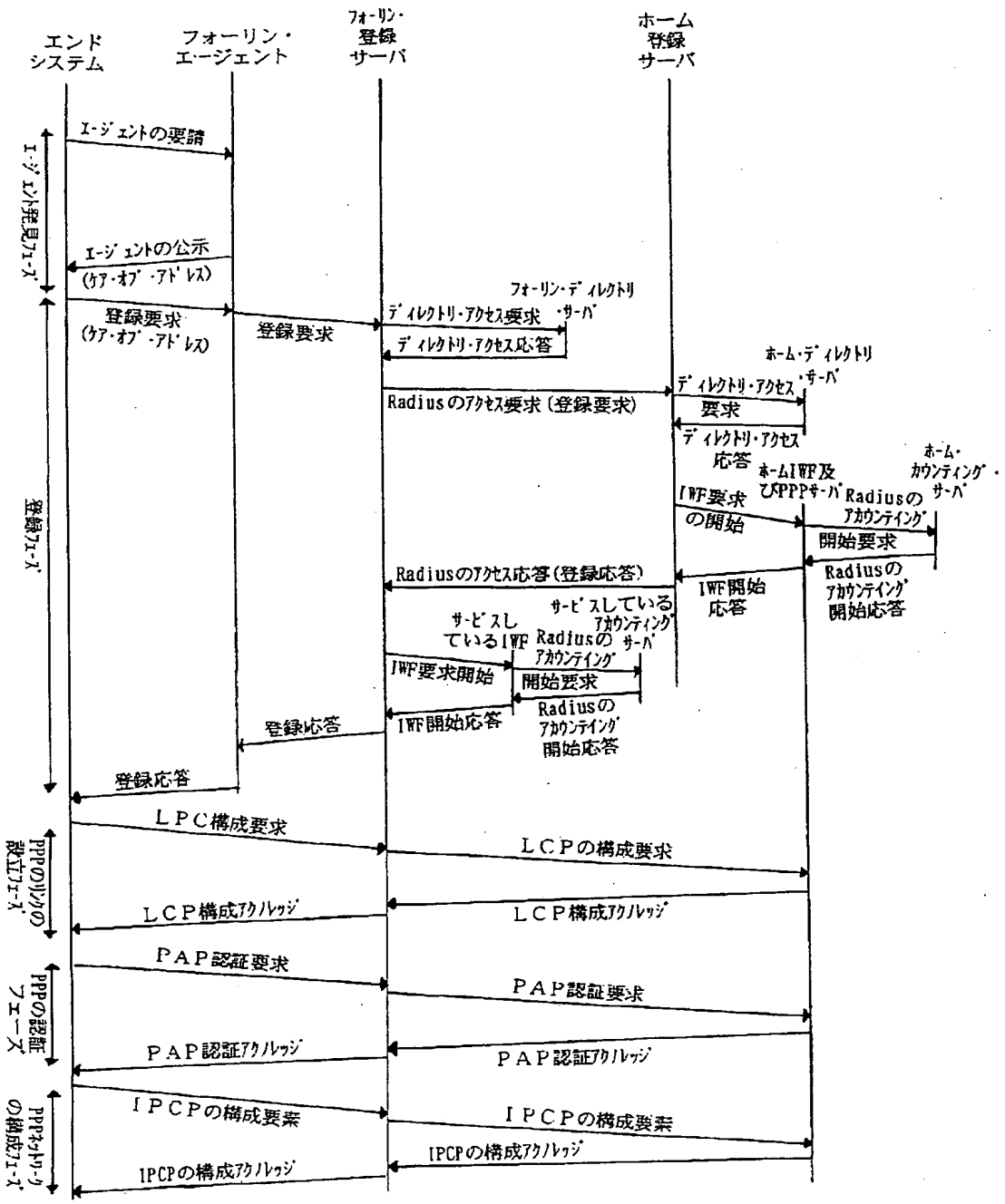
【図１６】


インターネット・サービス・プロバイダ A
PPPサーバ・エンド・システムAに対するPPPをターミネートする
ルータ
インターネット・サービス・プロバイダ B
PPPサーバ・エンド・システムBに対するPPPをターミネートする
ルータ
エンド・システムAに対するIWFファンクション
ルータ
エンド・システムBに対するIWFファンクション
ルータ
Xkunnel
Xkunnel
基地局
基地局
(エア・リンク)
(エア・リンク)
エンド・システム A
エンド・システム B
無線サービス・プロバイダ A
無線サービス・プロバイダ B

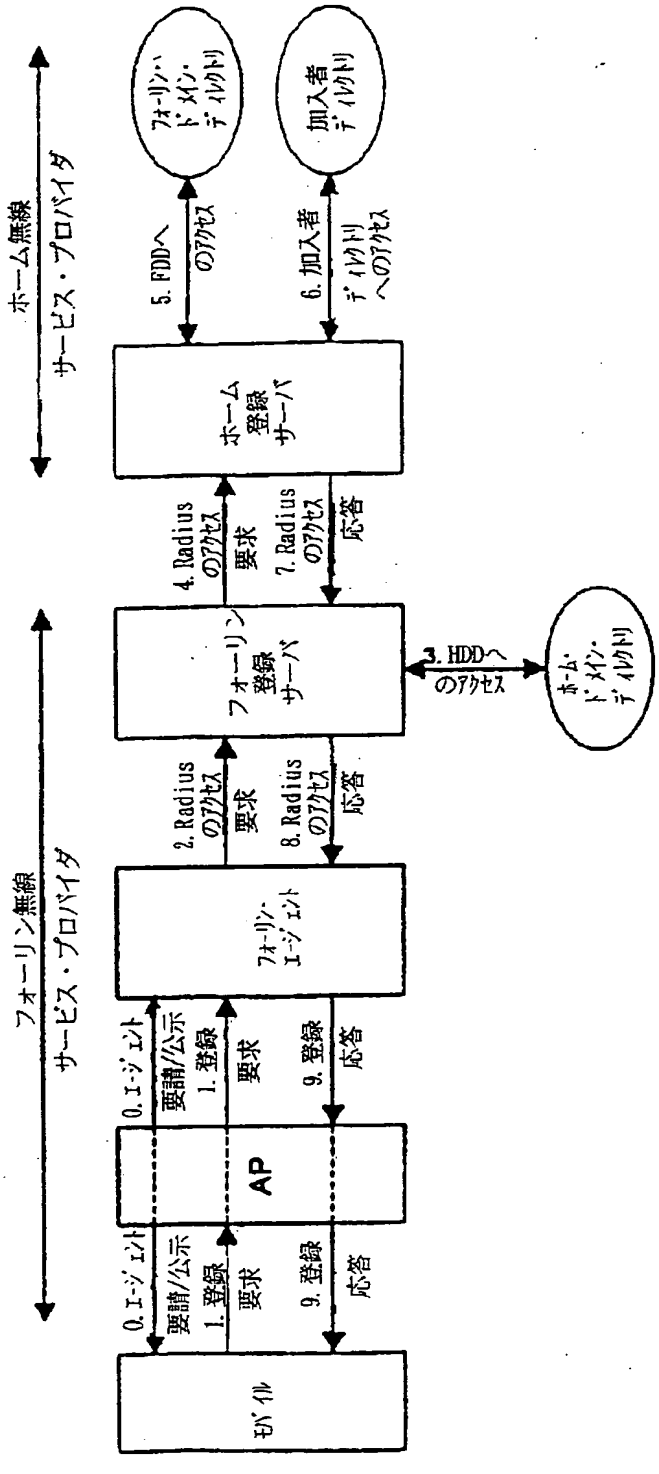
【図２３】


IP
PPP
L2TP
UDP
IP
T1/T3
ISP/インターネットPPPサーバ
IPネットワーク
パケットRTV/フォワ
RLP
Xkunnel
UDP
IP
LAN
L2TP
UDP
IP
LAN
IPネットワーク
ホームIWF
802.3
パケットポート
無線ハブ
フォーリン・エージェント
802.3
MAC
アクセス・ポイント
エア・リンク (f1)
エンド・システム
アプリケーション
UDP
TCP
IP
PPP
RLP
MAC

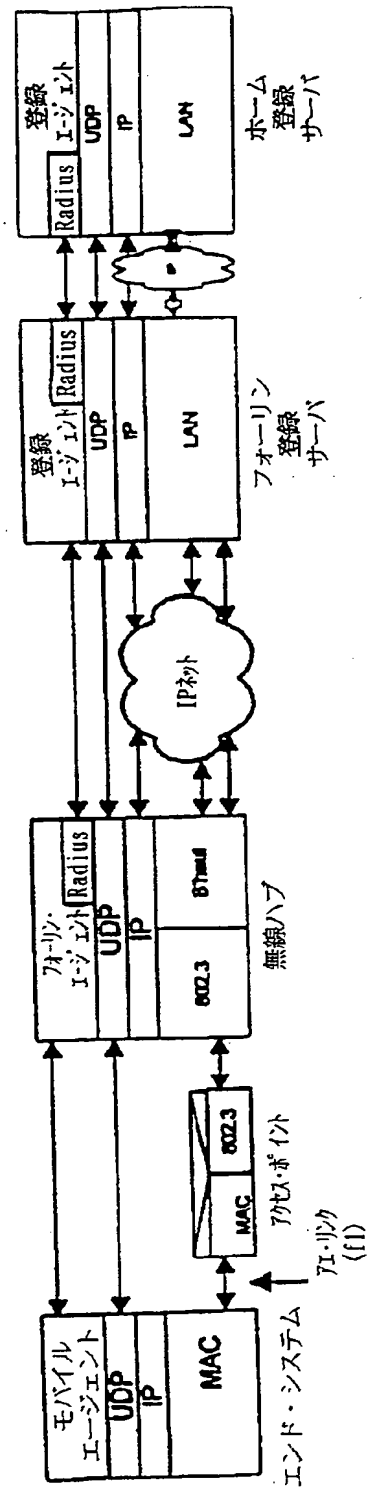
【図１７】


エンドシステム
フォーリン・エージェント
フォーリン・登録サーバ
ホーム登録サーバ
エージェント発見フェーズ
エージェントの要請
エージェントの公示
(ケア・オブ・アドレス)
登録フェーズ
登録要求(ケア・オブ・アドレス)
登録要求
フォーリン・ディレクトリ・サーバ
ディレクトリ・アクセス要求
ディレクトリ・アクセス応答
ホーム・ディレクトリ・サーバ
ディレクトリ・アクセス要求
ディレクトリ・アクセス応答
Radiusのアクセス要求(登録要求)
ホームIWF及びPPPサーバ
IWF要求の開始
ホーム・カウンティング・サーバ
Radiusのアカウンティング開始要求
Radiusのアカウンティング開始応答
IWF開始応答
Radiusのアクセス応答(登録応答)
サービスしているIWF
サービスしているアカウンティング・サーバ
Radiusのアカウンティング開始要求
IWF要求開始
Radiusのアカウンティング開始応答
IWF開始応答
登録応答
登録応答
PPPのリンクの設立フェーズ
LCP構成要求
LCPの構成要求
LCP構成アクノレッジ
LCP構成アクノレッジ
PPPの認証フェーズ
PAP認証要求
PAP認証要求
PAP認証アクノレッジ
PAP認証アクノレッジ
PPPネットワークの構成フェーズ
IPCPの構成要素
IPCPの構成要素
IPCPの構成アクノレッジ
IPCPの構成アクノレッジ

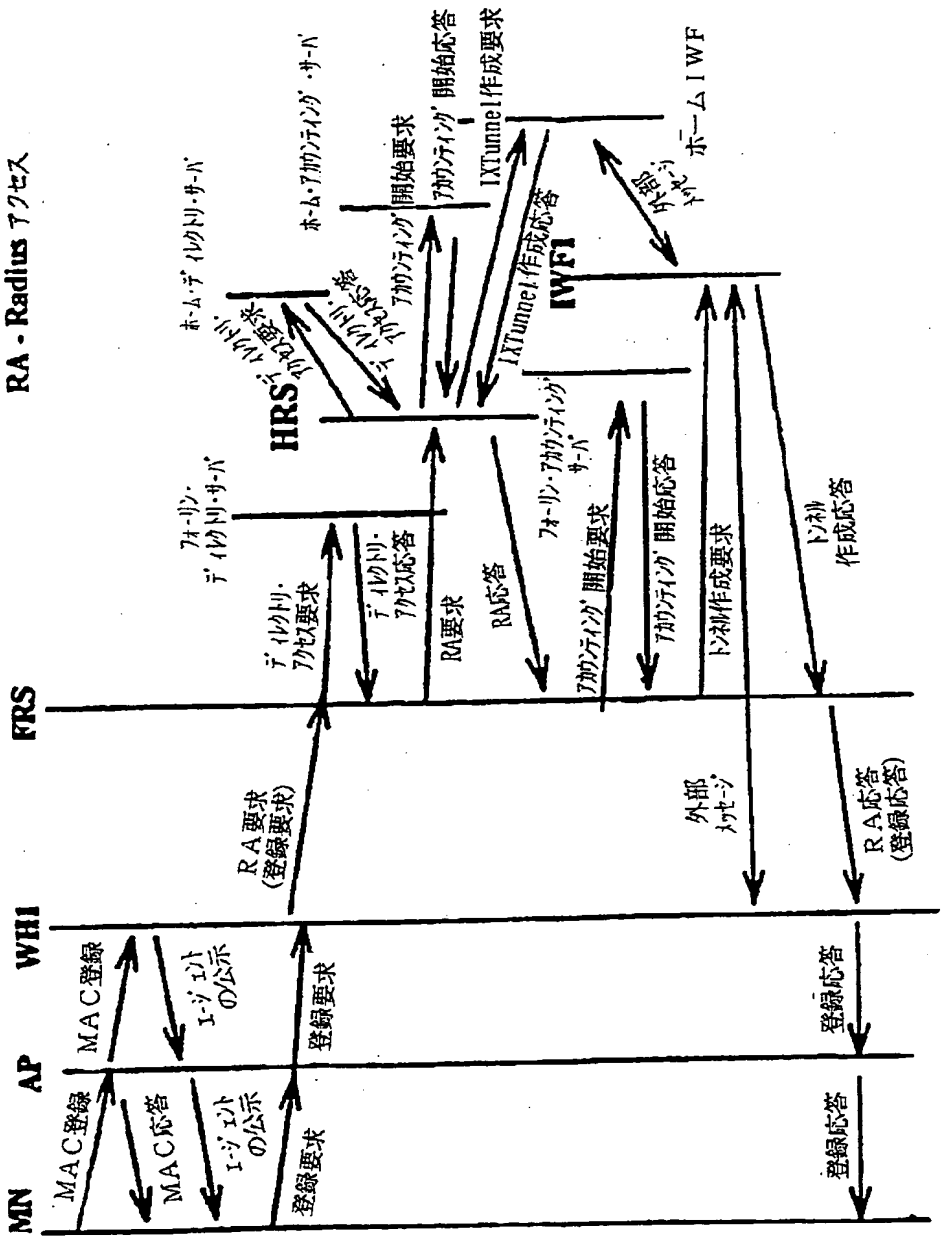
【図１９】


ホーム無線
サービス・プロバイダ
フォーリン無線
サービス・プロバイダ
フォーリン・ドメイン・ディレクトリ
加入者ディレクトリ
5. FDDへのアクセス
6. 加入者ディレクトリへのアクセス
ホーム登録サーバ
4. Radiusのアクセス
要求
7. Radiusのアクセス
応答
フォーリン登録サーバ
3. HDDへのアクセス
ホーム・ドメイン・ディレクトリ
2. Radiusのアクセス
要求
8. Radiusのアクセス
応答
フォーリン・エージェント
0. エージェント要請/公示
1. 登録要求
9. 登録応答
AP
モバイル

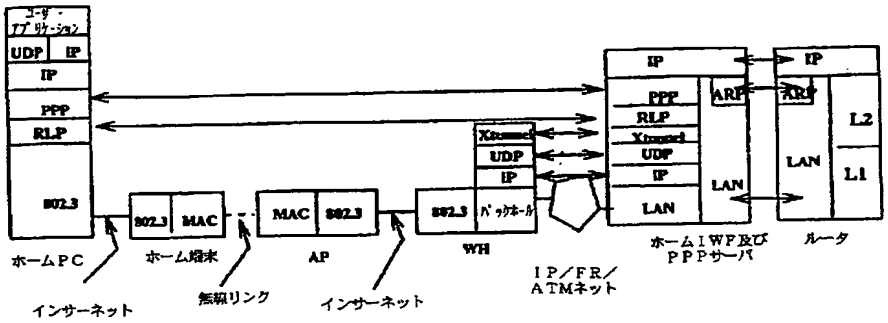
【図２４】


登録エージェント
Radius
UDP
IP
LAN
ホーム登録サーバ
フォーリン登録サーバ
IPネット
フォーリン・エージェント
802.3
Bluetooth
無線ハブ
MAC
アクセス・ポイント
エア・リンク(I1)
モバイル・エージェント
エンド・システム

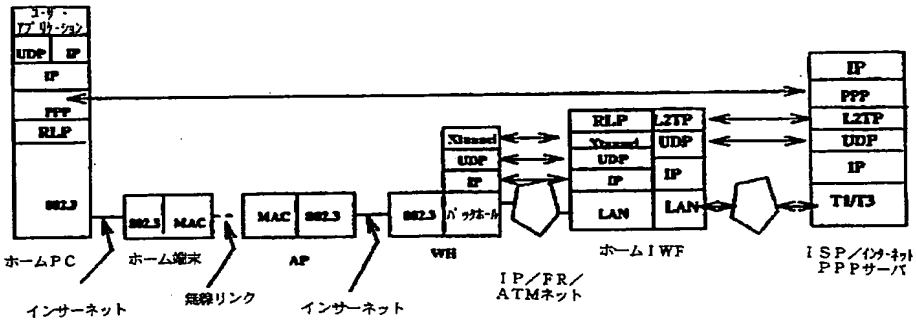
【図２７】


RA - Radius アクセス
MN
AP
WHI
FRS
HRS
IWF1
MAC登録
MAC応答
エージェントの公示
登録要求
RA要求 (登録要求)
RA応答 (登録応答)
登録応答
外部メッセージ
トンネル作成応答
トンネル作成要求
RA応答
RA要求
ディレクトリ・アクセス要求
ディレクトリ・アクセス応答
フォーリン・ディレクトリ・サーバ
ホーム・ディレクトリ・サーバ
ホーム・アカウンティング・サーバ
フォーリン・アカウンティング・サーバ
アカウンティング開始要求
アカウンティング開始応答
IXTunnel作成要求
IXTunnel作成応答
ホーム IWF

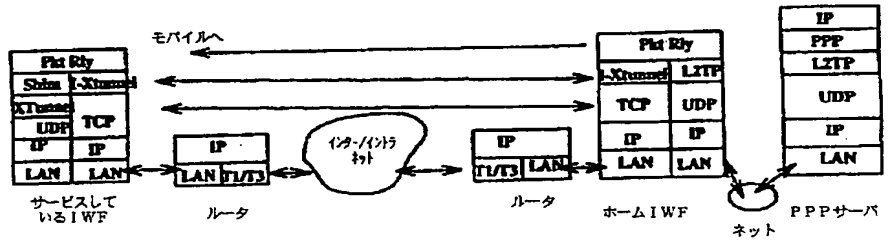
【図２８】



【図２９】

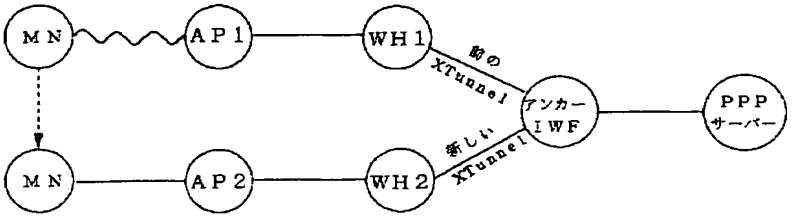


【図３１】

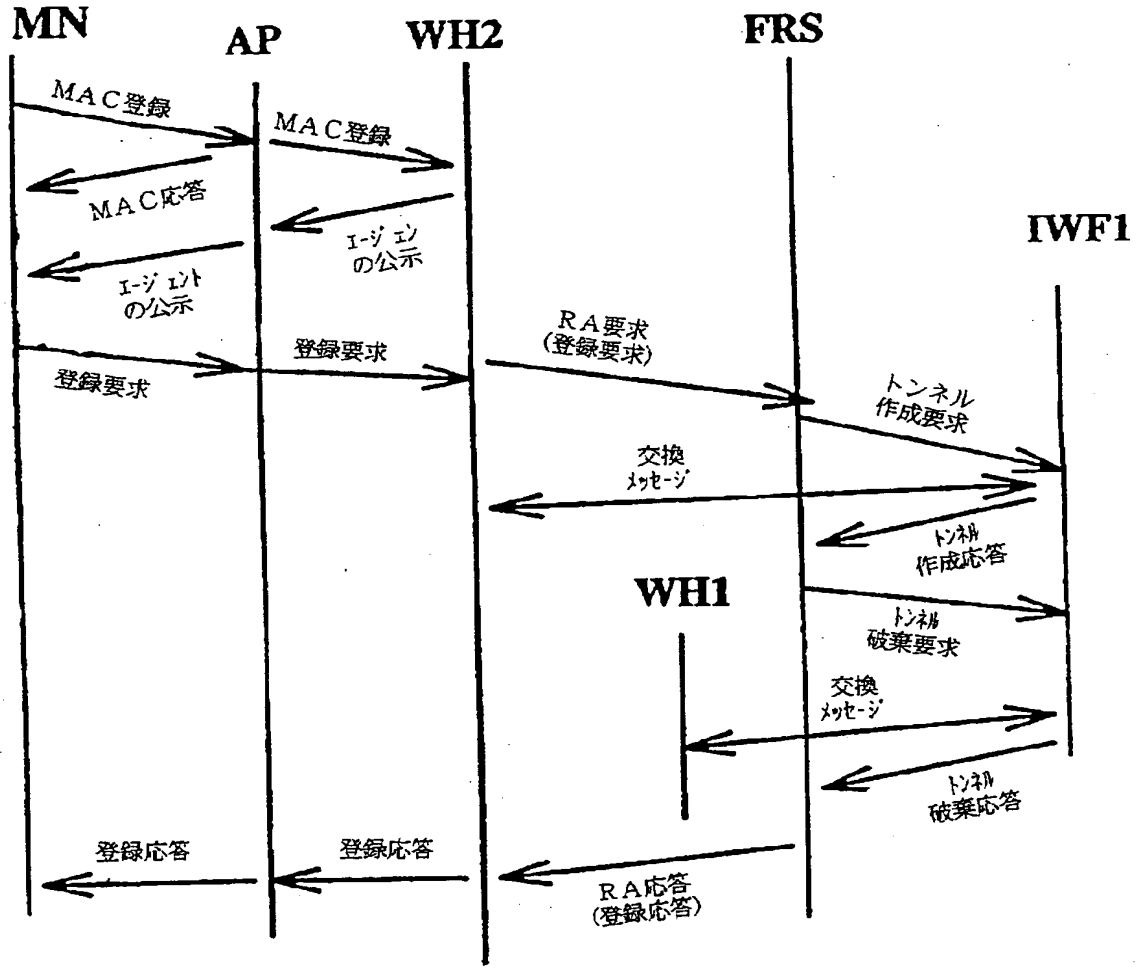


ホームＩＷＦとＰＰＰサーバが分かれている場合のロームしているモバイルに対するプロトコル・スタック

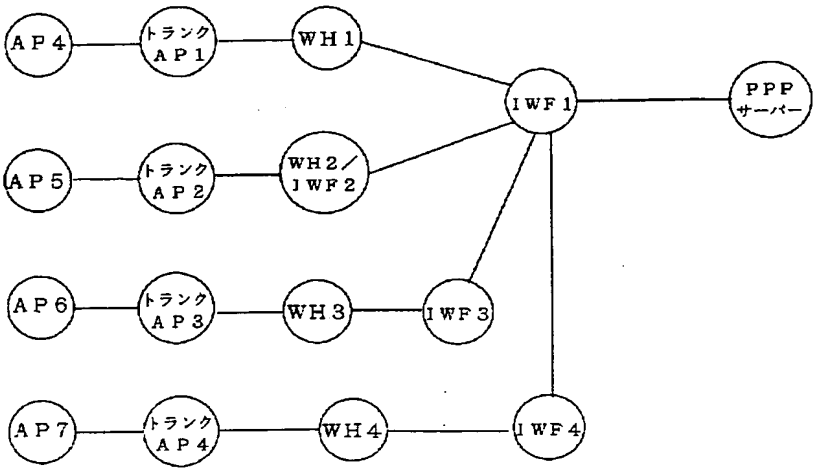
【図３９】



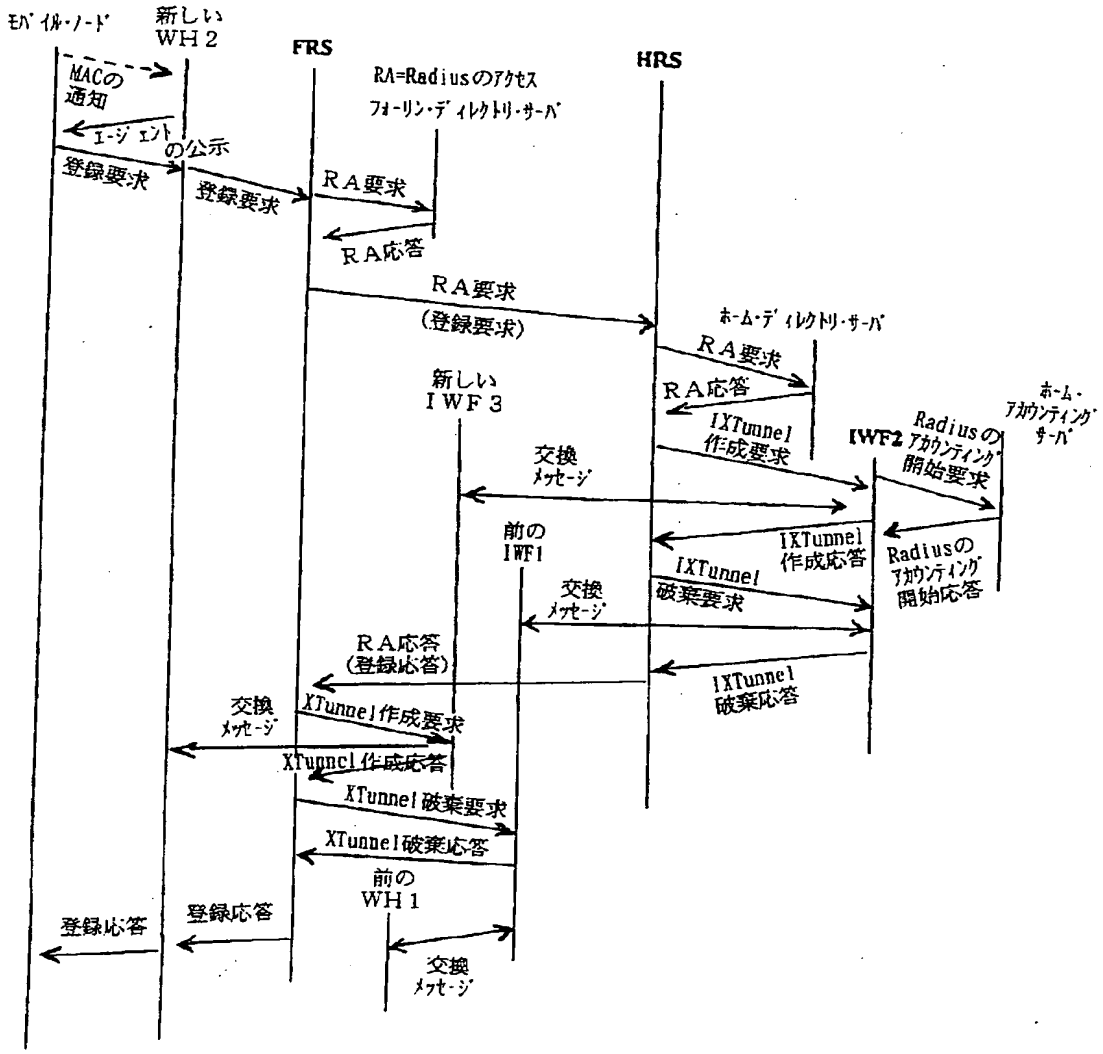
【図３３】


MN
AP
WH2
FRS
IWF1
WH1
MAC登録
MAC登録
MAC応答
エージェントの公示
エージェントの公示
登録要求
登録要求
RA要求
(登録要求)
トンネル作成要求
交換メッセージ
トンネル作成応答
トンネル破棄要求
交換メッセージ
トンネル破棄応答
登録応答
登録応答
RA応答
(登録応答)

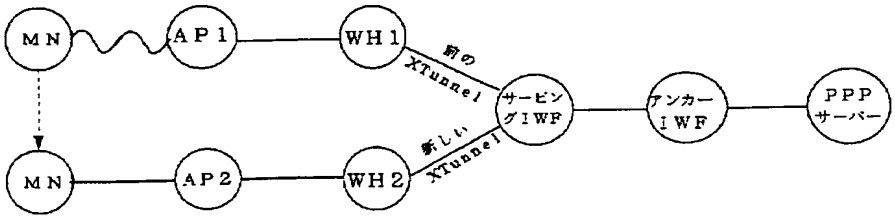
【図３８】


AP4
トランクAP1
WH1
IWF1
PPPサーバー
AP5
トランクAP2
WH2／IWF2
AP6
トランクAP3
WH3
IWF3
AP7
トランクAP4
WH4
IWF4

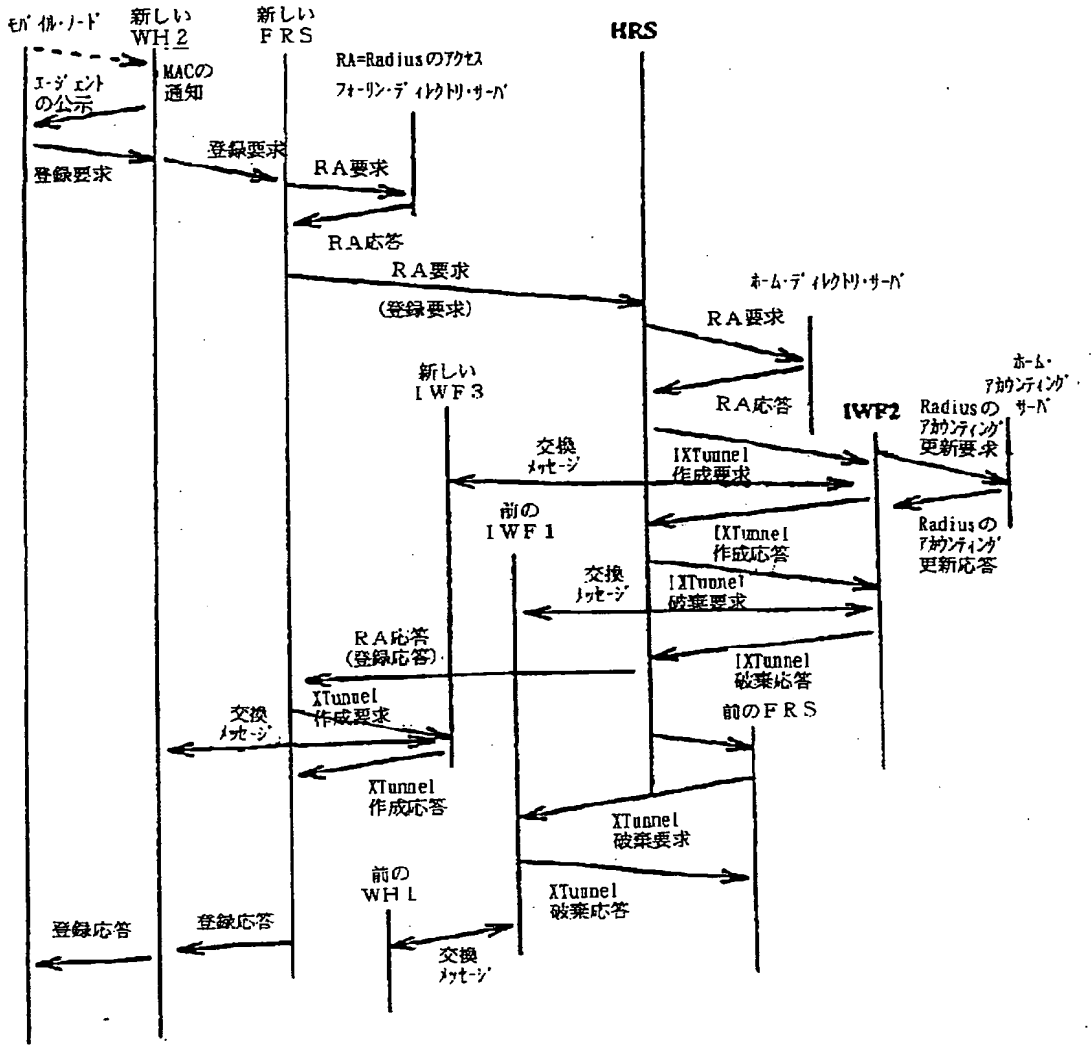
【図３４】


ﾓﾊﾞｲﾙ･ﾉｰﾄﾞ
新しい
WH２
FRS
RA=Radiusのｱｸｾｽ
ﾌｫｰﾘﾝ･ﾃﾞｨﾚｸﾄﾘ･ｻｰﾊﾞ
HRS
MACの
通知
ｴｰｼﾞｪﾝﾄ
の公示
登録要求
登録要求
RA要求
RA応答
RA要求
(登録要求)
ﾎｰﾑ･ﾃﾞｨﾚｸﾄﾘ･ｻｰﾊﾞ
RA要求
RA応答
新しい
IWF３
IXTunnel
作成要求
IWF2
Radiusの
ｱｶｳﾝﾃｨﾝｸﾞ
開始要求
ﾎｰﾑ･
ｱｶｳﾝﾃｨﾝｸﾞ
ｻｰﾊﾞ
交換
ﾒｯｾｰｼﾞ
前の
IWF1
IXTunnel
作成応答
Radiusの
ｱｶｳﾝﾃｨﾝｸﾞ
開始応答
IXTunnel
破棄要求
交換
ﾒｯｾｰｼﾞ
RA応答
(登録応答)
IXTunnel
破棄応答
交換
ﾒｯｾｰｼﾞ
XTunnel作成要求
XTunnel作成応答
XTunnel破棄要求
XTunnel破棄応答
前の
WH１
登録応答
登録応答
交換
ﾒｯｾｰｼﾞ

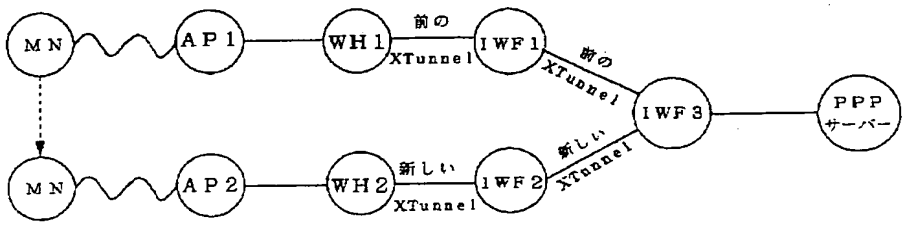
【図４０】


ＭＮ
ＡＰ１
ＷＨ１
前の
XTunnel
サービン
グＩＷＦ
アンカー
ＩＷＦ
ＰＰＰ
サーバー
ＭＮ
ＡＰ２
ＷＨ２
新しい
XTunnel

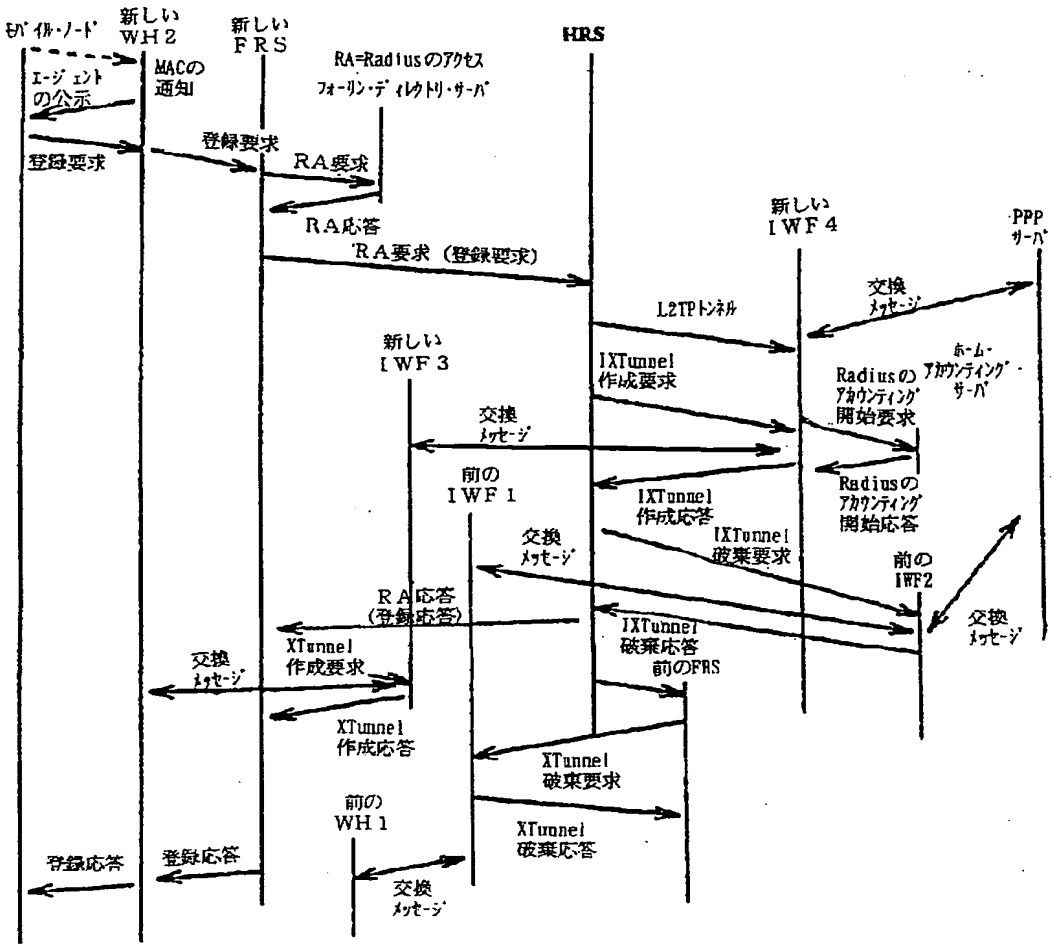
【図３５】


ﾓﾊﾞｲﾙ･ﾉｰﾄﾞ
新しい WH2
新しい FRS
HRS
RA=Radiusのｱｸｾｽ ﾌｫｰﾘﾝ･ﾃﾞｨﾚｸﾄﾘ･ｻｰﾊﾞ
ﾎｰﾑ･ﾃﾞｨﾚｸﾄﾘ･ｻｰﾊﾞ
新しい IWF3
前の IWF1
IWF2
ﾎｰﾑ･ｱｶｳﾝﾃｨﾝｸﾞ･ｻｰﾊﾞ
ｴｰｼﾞｪﾝﾄの公示
MACの通知
登録要求
登録要求
RA要求
RA応答
RA要求
(登録要求)
RA要求
RA応答
交換ﾒｯｾｰｼﾞ
IXTunnel 作成要求
Radiusの ｱｶｳﾝﾃｨﾝｸﾞ 更新要求
IXTunnel 作成応答
Radiusの ｱｶｳﾝﾃｨﾝｸﾞ 更新応答
交換ﾒｯｾｰｼﾞ
IXTunnel 破棄要求
RA応答 (登録応答)
IXTunnel 破棄応答
XTunnel 作成要求
交換ﾒｯｾｰｼﾞ
前のFRS
XTunnel 作成応答
XTunnel 破棄要求
前の WHL
XTunnel 破棄応答
登録応答
登録応答
交換ﾒｯｾｰｼﾞ

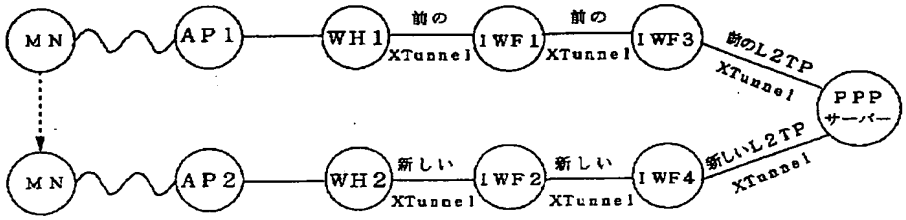
【図４１】


MN
AP1
WH1
前の XTunnel
IWF1
前の XTunnel
IWF3
PPP サーバー
MN
AP2
WH2
新しい XTunnel
IWF2
新しい XTunnel

【図３６】



【図４２】



フロントページの続き

(51) Int. Cl. 6	識別記号	F I	
H04L 12/56		H04L 11/00	310C
H04M 3/00			F
11/00	303	11/20	102D

(72)発明者 ギリシュ ライ
アメリカ合衆国 60103 イリノイズ，バートレット，レディ スミス ロード 523